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

IIROC NOTICE

Rules Notice
Guidance Note
Dealer Member Rules [IIROC Rules]

Please distribute internally to:
Legal and Compliance
Operations
Retail
Senior Management
Training

Contact:

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

Suzanne Lasrado
Senior Manager, Financial & Operations Compliance
Telephone: 416.943.5880
e-mail: slasrado@iiroc.ca

19-0195
November 14, 2019

Frequently Asked Questions – Mandatory Cybersecurity Incident Reporting

Executive Summary

IIROC is publishing Frequently Asked Questions about the mandatory reporting of a cybersecurity incident by Dealer Members (**Dealers**) to IIROC set out in Rule 3100,1.B, 1.1 [subsection 3703(1) and clause 3703(2)(vii) of the IIROC Rules] (the **Cybersecurity Reporting Obligation**).[1] We intend to periodically update this document as necessary.[2]

[1] In this guidance, when referencing specific subsections of the Cybersecurity Reporting Obligation, we will cite the Dealer Member Rule (**DMR**) sections with the corresponding IIROC Rules section in square brackets. See Notice 19-0144 – IIROC Dealer Member Plain Language Rule Book Implementation. Upon implementation of the IIROC Rules, we will remove references to the DMRs.

[2] We also intend to publish this Frequently Asked Questions on an "FAQ" subpage of the IIROC website, which will be periodically updated.

#	Question	Answer
1.	How do Dealers know if they should report a cybersecurity incident to IIROC?	Dealers should assess whether the cybersecurity incident falls within the definition of "cybersecurity incident".[3] We drafted the definition of cybersecurity incident in a flexible manner to accommodate the evolving nature and variety of cybersecurity threats. Cybersecurity incidents may have a different impact on a Dealer's operations depending on the nature of the Dealer's business model and the type of cybersecurity incident. The definition includes breaches that: • involve personal information and may be reportable under the reporting obligations of the *Privacy Information Protection and Electronic Documents Act* (**PIPEDA**), • affect a Dealer's ability to meet its obligations to its clients and capital market counterparties, and • affect both individuals and non-individuals. Dealers are required to report a cybersecurity incident if any of the listed outcomes[4] take place or if the Dealer determines there is a reasonable likelihood of those outcomes taking place.
2.	How do Dealers assess the reasonable likelihood of substantial harm to any *person?*	Dealers should use judgment to assess whether an incident has a reasonable likelihood of resulting in any of the outcomes listed in Rule 3100, I.B 1.1, section (1)(i) to (iv) [clause 3703(1)(i)-(iv) of the IIROC Rules]. The probability of substantial harm to any person may include harm to a non-individual client and may relate to more than just the misuse of personal information.
3.	How do Dealers assess the "materiality" of the impact of a cybersecurity incident on any part of my normal	Materiality will vary between Dealers of different sizes and business models. Dealers should exercise judgment to determine what constitutes a "material impact" on a Dealer's normal operations.

[3] As defined in Rule 3100, I.B. 1.1, section (1) [subsection 3703(1) of the IIROC Rules].
[4] Per Rule 3100, I.B 1.1, section (1)(i) to (iv) [clause 3703(1)(i)-(iv) of the IIROC Rules]:
(i) substantial harm to any person,
(ii) a material impact on any part of the normal operations of the Dealer,
(iii) invoking the Dealer's business continuity plan or disaster recovery plan, or
(iv) the Dealer Member being required to provide notice under other regulatory obligations.

#	Question	Answer
	operations?	
4.	Does a Dealer need to report a cybersecurity incident that takes place at a material third-party information systems service provider?	The mere fact that a cybersecurity incident takes place at a service provider does not exclude the incident from reporting. A Dealer should evaluate its "information system" or "information stored on such information system" to include elements that may be supplied by third-party service providers. The other components of the definition of "cybersecurity incident" must also be present to trigger reporting.
5.	Does a Dealer need to report a cybersecurity incident that slows down its website or internal systems?	An incident that slows down a Dealer's website or internal systems needs to be reported to IIROC only if it meets the criteria listed in Rule 3100, I.B 1.1, section (1)(i) to (iv)[clause 3703(1)(i)-(iv)]. Accordingly, if the incident slowed down a Dealer's internal system in a manner that had a material impact on any part of a Dealer's normal operations, then we would expect the Dealer to report to IIROC.
6.	Whom should a Dealer contact if it has a cybersecurity incident to report? What happens after a Dealer reports the incident to IIROC?	A Dealer should contact its Financial & Operations Compliance (**FinOps**) relationship manager. We will arrange a meeting, generally on the same day, to discuss the preliminary details of the cybersecurity incident and next steps. The meeting will include the following: • Senior management in FinOps, • Senior management in the IIROC Information Technology and Information Security department, and • the Chief Executive Office, Chief Financial Officer, Chief Information Officer/ Chief Information Security Office and Chief Compliance Officer of a Dealer.
7.	A Dealer has experienced a cybersecurity incident. What does it do next?	A Dealer should follow its incident response and management plan. If it does not have a plan, we strongly recommend that the Dealer consult its cybersecurity insurance provider or engage the services of cybersecurity professionals and external legal counsel for guidance on how to proceed and best protect the Dealer and its clients. A Dealer's incident response and management plan should include its reporting obligations.

#	Question	Answer
8.	What information do Dealers need to provide to IIROC in the first three days of discovering a cybersecurity incident?	Within three days from discovering a cybersecurity incident, a Dealer must, at a minimum, report the following: • a description of the cybersecurity incident, • the date the cybersecurity incident was discovered and the date or time period during which the cybersecurity incident occurred, • a preliminary assessment of the cybersecurity incident, including the risk of harm to any person or impact on a Dealer's operations, • a description of immediate incident response steps a Dealer has taken, and • contact information for an individual who can answer follow-up questions. However, if a Dealer has additional information, it should share this with IIROC. The three-day report is meant to reflect only a preliminary assessment of the cybersecurity incident. The three-day report is not meant to reflect material insights respecting assessment or remediation. We recognize that a Dealer may not have a complete analysis within three calendar days following discovery of the cybersecurity incident. We expect Dealers to submit the best information available to it at the time of reporting.
9.	A Dealer has identified a possible cybersecurity incident but is not sure if the incident meets the definition of cybersecurity incident to trigger reporting. Does the Dealer still need to contact IIROC within three days?	We recommend that a Dealer contacts its FinOps relationship manager for guidance if there is any uncertainty.
10.	After a Dealer has reported the cybersecurity incident to IIROC, it concludes that no	No. A notification to IIROC advising us of this is sufficient. However, in order to protect Dealers from legal and regulatory liability, we strongly recommend that Dealers confirm with

#	Question	Answer
	cybersecurity incident, as defined in the IIROC Rules, occurred. Does the Dealer still need to provide a 30-day incident investigation report (the **30-day Report)**?	external legal counsel and cybersecurity professionals that: • the incident did not result in a breach of personal information, • a Dealer's information systems or information stored on such a system were not materially impacted, and any action taken is sufficient and complies with all applicable laws, including privacy laws.
11.	What is the difference between the three-day and 30-day Report?	The three-day report is a brief snapshot of core information provided by a Dealer immediately following discovery of a cybersecurity incident. The 30-day Report is a more detailed report that a Dealer produces after more fully investigating a cybersecurity incident.
12.	What if a Dealer needs more than 30 days to submit the 30-day Report?	If a Dealer needs more time, it should notify its FinOps relationship manager and let them know: • why the Dealer needs more time, • when the Dealer expects the 30-day Report to be completed, and • when the Dealer will submit the 30-day Report. If IIROC agrees to grant an extension, a Dealer should keep IIROC up to date regarding the status of the Dealer's investigation and the actions the Dealer takes.
13.	What information does a Dealer need to provide in the 30-day Report?	The 30-day Report should include all relevant and pertinent information that would help a Dealer determine the nature, extent, scope, impact and root cause of the cybersecurity incident. The report should also include actions taken to recover, respond and remediate. At a minimum, a Dealer must include the following in its report: (a) description of the cause of the cybersecurity incident, (b) an assessment of the scope of the cybersecurity incident, including the number of persons harmed and the impact on a Dealer's operations, such as: • the number of devices affected,

#	Question	Answer
		• the number of business days that a Dealer's operations were impacted, • estimated costs to address the cybersecurity incident, including whether the Dealer has cybersecurity insurance and the amount of the deductible, • what information on a Dealer's information system was affected and if it included client data, (c) details of the steps a Dealer has taken to mitigate the risk of harm to persons and impact on a Dealer's operations, including if a Dealer notified any other regulators or external parties, (d) details of the steps a Dealer took to remediate any harm to any person, including if a Dealer engaged any legal counsel, and (e) actions a Dealer has taken to improve its cybersecurity incident preparedness.
14.	Does a Dealer need to submit separate reports for a cybersecurity incident involving the same clients if it has different divisions (such as a wealth management and securities division) that are each affected by the cybersecurity incident?	A Dealer would need to submit one report that includes information referencing both divisions if the cybersecurity incident arose from the same act to gain unauthorized access to, disrupt or misuse a Dealer's information system, or information stored on the Dealer's information system. The Cybersecurity Reporting Obligation defines cybersecurity incident in terms of the originating unauthorized act, rather than in terms of the impacted clients.
15.	When should a Dealer engage external forensics auditors? Can a Dealer use its own internal IT staff or managed services provider to investigate the root cause of the cybersecurity incident?	We recommend using external forensics auditors if a Dealer: • lacks the specialized knowledge, tools and resources needed to fully investigate the cybersecurity incident, and • seeks to manage potential conflicts of interest. Identifying the root cause of a cybersecurity incident is a critical step in ensuring that the cybersecurity incident does not re-occur, and that a Dealer has effectively addressed any potential

#	Question	Answer
		ongoing risks associated with the cybersecurity incident.
16.	How will a Dealer know if the incident has been closed by IIROC?	We will inform a Dealer when we close our review of the cybersecurity incident and require no further reporting. However, if a Dealer later obtains information related to the cybersecurity incident, it must contact IIROC with these details.
17.	What will IIROC do with the information reported to IIROC respecting a cybersecurity incident?	We plan to share with the Dealer community: • general cybersecurity incident information periodically, depending on the volume and nature of cybersecurity incidents that Dealers report to IIROC, and • information about cybersecurity incidents reported to IIROC to sufficiently describe the nature of the incident and risk to other Dealers or investors. We will not disclose the names of the Dealers who have reported cybersecurity incidents to other Dealers or the public. We will anonymize any information about reported cybersecurity incidents that we share with the public or other Dealers.

1. Applicable Rules

Rules this Guidance Note relates to are:

- Dealer Member Rule 3100(1)(B)1.1 [subsection 3703(1) and clause 3703(2)(vii) of the IIROC Rules].

2. Related Documents

This Guidance note was published along with Notice of Approval/Implementation 19-0194.