IIROC INTRODUCES MANDATORY REPORTING OF CYBERSECURITY INCIDENTS FOR DEALERS

Posted on December 9, 2019

Categories: Insights, Publications

On November 14, 2019, the Investment Industry Regulatory Organization of Canada ("**IIROC**") amended its Dealer Member Rules (the "**Rules**") to require mandatory reporting by dealer members ("**Dealers**") that suffer a cybersecurity incident or breach (the "**Amendments**"). The Amendments are the latest initiative undertaken by IIROC in its ongoing focus on proactively addressing the cybersecurity risk exposure of its Dealers. For this reason, IIROC plans to share the information reported with the Dealer community on an anonymized basis to allow Dealers to understand the nature of risks they face and how they can protect themselves and their clients.

IIROC's mandatory reporting requirements are similar to the requirements of the Office of the Superintendent of Financial Institutions ("**OSFI**") which were introduced earlier this year, and which apply to some Dealers.

However, IIROC's reporting requirements are broader than the reporting requirements under the federal Personal Information Protection and Electronic Documents Act ("**PIPEDA**"), which also apply to some Dealers. IIROC's broader reporting requirements support its mission to protect investors, strengthen market integrity and support healthy Canadian capital markets. You can read more about OSFI reporting requirements in our February 2019 bulletin and PIPEDA reporting requirements in our November 2018 bulletin.

The Amendments require Dealers to report prescribed information regarding a cybersecurity incident to IIROC in two stages:

1. A Dealer must file an initial report with IIROC describing the cybersecurity incident within three (3) calendar days of discovering it;
2. The Dealer must subsequently submit a detailed incident investigation report within thirty (30) calendar days of the incident.

If a Dealer fails to comply with the reporting obligation, IIROC can impose significant monetary penalties or other sanctions.

What Triggers the Reporting Obligation?

A Dealer's reporting obligation is triggered by the Dealer's discovery of a cybersecurity incident.

Cybersecurity incident

Under the Rules, a cybersecurity incident includes any act to gain unauthorized access to, disrupt, or misuse a Dealer's information system, or information stored on such system, which has resulted in, or has a reasonable likelihood of resulting in:

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 or disaster recovery plan; or
iv. the Dealer being required under any applicable laws to provide notice to any government body, securities regulatory authority or other self-regulatory organization.

IIROC has indicated that the above definition of a cybersecurity incident is intended to be flexible. IIROC expects Dealers to exercise their discretion when determining whether a cybersecurity event meets the reporting threshold.

Dealers should be aware that they are not exempt from the reporting obligation imposed by the Amendments solely because a cybersecurity incident has been experienced by a third-party information systems service provider. Cybersecurity incidents experienced by third parties will trigger a Dealer's reporting obligation if: (i) those third parties are part of that Dealer's "information system"; and (ii) the other elements of the definition of a "cybersecurity incident" are met. We recommend that Dealers consider including provisions in their contracts with the third parties that oblige third parties to: (i) notify Dealers of a cybersecurity incident within 24 hours; and (ii) provide Dealers with all relevant information about the incident. This will help Dealers meet their reporting obligation.

What Information Must be Included in an "Initial Report" and "Incident Investigation Report"?

Initial report

The initial report that is required to be filed by a Dealer within three (3) calendar days of that Dealer's discovery of a cybersecurity incident must include the following information:

i. a description of the cybersecurity incident;
ii. the date on which or time period during which the cybersecurity incident occurred and the date it was discovered by the Dealer;
iii. a preliminary assessment of the incident, including the risk of harm to any person and/or impact on the operations of the Dealer;

iv. a description of the immediate incident response steps the Dealer has taken to mitigate the risk of harm to persons and impact on its operations; and
v. the name and contact information of an individual who can answer any follow-up questions from IIROC on behalf of the Dealer.

IIROC recognizes that a Dealer may not have completed a full analysis of a cybersecurity incident within three (3) calendar days. Accordingly, IIROC does not expect an initial report to reflect material insights respecting the assessment or remediation of a cybersecurity incident. Rather, an initial report is intended to be a preliminary snapshot of the core information relevant to the cybersecurity incident.

Dealers should note that while the information listed above is the minimum information required, IIROC expects Dealers to include additional information about a cybersecurity incident in their initial reports to the extent such additional information is available.

Incident investigation report

An incident investigation report, which is required to be filed by a Dealer within thirty (30) calendar days of that Dealer's discovery of a cybersecurity incident, must include the following information:

i. a description of the cause of the cybersecurity incident;
ii. an assessment of the scope of the cybersecurity incident, including the number of persons harmed and the impact on the operations of the Dealer;
iii. details of the steps the Dealer took to mitigate the risk of harm to persons and impact on its operations;
iv. details of the steps the Dealer took to remediate any harm to any persons; and
v. actions the Dealer has or will take to improve its cybersecurity incident preparedness.

IIROC expects that an incident investigation report will include all relevant and pertinent information that would help a Dealer determine the nature, extent, scope, impact and root cause of a cybersecurity incident. If a Dealer requires more than thirty (30) days to file an incident investigation report, it should notify its IIROC relationship manager.

After filing an initial report, if a Dealer subsequently determines that no cybersecurity incident has occurred, the Dealer does not need to file an incident investigation report. IIROC recommends that Dealers contact external legal counsel and cybersecurity professionals before making such a determination.

How External Legal Counsel Can Assist Dealers in the Event of a Cybersecurity Incident

IIROC recommends that Dealers should follow their incident response and management plan once they discover a cybersecurity incident. If a Dealer does not have an incident response and management plan, IIROC

recommends consultation with external legal counsel for assistance to ensure that it protects itself and its clients.

Dealers should be aware that, when a cybersecurity incident occurs, they may be subject to additional reporting requirements under other privacy laws and regulations. External legal counsel can also advise on these other reporting requirements, and assist organizations to meet all applicable legal obligations.

by Lyndsay Wasser, Chiedza Museredza, Chris Tworzyanski

A Cautionary Note

The foregoing provides only an overview and does not constitute legal advice. Readers are cautioned against making any decisions based on this material alone. Rather, specific legal advice should be obtained.