Cybersecurity Bulletin

November 2019

IIROC Imposes Mandatory Reporting of Cybersecurity Incidents for Regulated Investment Firms

On November 14, 2019, the Investment Industry Regulatory Organization of Canada (IIROC) – the national self-regulatory organization that oversees investment dealers and their trading activity in Canadian markets – published a notice of amendments to its Rule 3100 and Rule 3703 to require mandatory reporting of cybersecurity incidents by IIROC-regulated investment firms. The amended rules, which came into effect immediately on publication of the notice, require firms to provide IIROC with an initial report within three days of discovering a reportable cybersecurity incident and a comprehensive investigation report within 30 days of discovering the incident.

The IIROC cybersecurity incident reporting obligations apply in a wider range of circumstances than similar reporting obligations under Canadian personal information protection laws. Furthermore, the reporting obligations apply concurrently with other reporting obligations to which IIROC-regulated investment firms might also be subject, such as the technology and cybersecurity incident reporting obligations imposed by the Office of the Superintendent of Financial Institutions. IIROC-regulated investment firms should immediately assess their readiness to comply with these new reporting obligations and make appropriate changes to their systems, policies and procedures, and contracts with information technology service providers.

Previous Cybersecurity Guidance

Over the past few years, Canadian investment and financial industry regulators have emphasized the importance of cybersecurity, and have issued guidance to help regulated firms improve their cybersecurity maturity and manage cyber risks. For example:

- **IIROC:** In December 2015, IIROC published a *Cybersecurity Best Practices Guide* and a *Cyber Incident Management Planning Guide* to help investment dealers manage cybersecurity risks and respond to cyber incidents. In March 2018, IIROC published a notice warning investment dealers of the increasing frequency and sophistication of cybersecurity incidents, and asking dealers to voluntarily report cybersecurity incidents to IIROC.
- **MFDA:** In May 2016, the Mutual Fund Dealers Association of Canada published *Compliance Bulletin No. 0690-C-Cybersecurity* to help its member dealers manage cybersecurity risks.
- **CSA:** In October 2017, the Canadian Securities Administrators (CSA) published *Staff Notice 33-321 Cyber Security and Social Media* to report on a survey of cybersecurity and social media practices by firms registered to trade securities or to advise clients regarding securities, and to provide guidance regarding cybersecurity and social media practices. The Staff Notice supplemented the CSA's 2016 *Staff Notice 11-332 Cyber Security*.

- **OSFI:** In October 2013, the Office of the Superintendent of Financial Institutions Canada (OSFI) issued its *Cyber Security Self-Assessment Guidance* to help federally regulated financial institutions manage cyber risks. In January 2019, OSFI issued an *Advisory* setting out OSFI's expectations for federally regulated financial institutions regarding the prompt (within 72 hours) reporting of "high or critical severity" technology and cybersecurity incidents.

For more information, see BLG bulletins *Cybersecurity Guidance from Investment Industry Organization* (January 2016), *Cybersecurity Guidance from Investment Industry Organization* (May 2016), *Cybersecurity Guidance from Canadian Securities Administrators*, *OSFI Issues Advisory on Technology and Cybersecurity Incident Reporting*, and *Investment Funds Institute of Canada Issues Cybersecurity Guide*.

IIROC Rules – Mandatory Reporting of Cybersecurity Incidents

Background

IIROC's amended rules for mandatory reporting of cybersecurity incidents were first proposed by IIROC in an April 2018 *notice*, which detailed and discussed the proposed amended rules. The notice explained that the purpose of requiring mandatory reporting of cybersecurity incidents by IIROC's dealer members (dealers) is to allow IIROC to: (1) provide immediate support to the dealer responding to a cybersecurity incident; (2) alert other dealers of threats and share best practices for incident preparedness; (3) evaluate trends and develop comprehensive insight regarding cybersecurity; and (4) promote confidence in the dealer and the integrity of the market.

The notice invited public comment on the proposed amended rules. IIROC has summarized the comments it received, and its responses to those comments, in its April 2018 *notice* and a *Response to Public Comments*.

As a result of the public comment process, IIROC made minor changes to the proposed amended rules and published a guidance note, *Frequently Asked Questions – Mandatory Cybersecurity Incident Response*, to provide guidance for compliance with the amended rules.

Details of Amended Rules

Amended Rule 3100 and Rule 3703 came into effect immediately when published on November 14, 2019. Following is a summary of key aspects of the amended rules.

- **Cybersecurity Incident:** The rules define "cybersecurity incident" as including any act to gain unauthorized access to, disrupt or misuse a dealer's information system, or information stored on an information system, that has resulted in, or has a reasonable likelihood of resulting in, any of the following outcomes: (1) substantial harm to any person (which includes a natural person or legal entity); (2) a material impact on any part of the dealer's normal operations; (3) invoking the dealer's business continuity plan or disaster recovery plan; or (4) the dealer being required by any applicable law to provide notice to any government body, securities regulatory authority or other self-regulatory organization.
- **Initial Report:** The rules require a dealer to provide a written incident report to IIROC within three calendar days after the dealer discovers a cybersecurity incident. The report must include: (1) a description of the cybersecurity incident; (2) the date or period during which the cybersecurity incident occurred and the date it was discovered by the dealer; (3) a preliminary assessment of the cybersecurity incident, including the risk of harm to any person and impact on the operations of the dealer; (4) a description of immediate incident response steps the dealer has taken to mitigate the risk of harm to persons and the impact on the dealer's operations; and (5) the name of and contact information for an individual who can answer IIROC's follow-up questions.
- **Comprehensive Investigation Report:** The rules require a dealer to provide a comprehensive, written incident investigation report to IIROC within 30 days, or a longer period agreed to by IIROC, after the dealer discovers a cybersecurity incident. The report must include: (1) a description of the cause of the cybersecurity incident; (2) an assessment of the scope of the cybersecurity incident, including the number of persons harmed and the impact on the dealer's operations; (3) details of the steps the dealer took to mitigate the risk of harm to persons and impact on the dealer's operations; (4) details of the steps the dealer took to remediate any harm to any persons; and (5) actions the dealer has or will take to improve its cybersecurity incident preparedness.

A dealer's failure to comply with the cybersecurity incident reporting obligations could result in IIROC imposing potentially significant financial penalties or other sanctions on the dealer.

IIROC's Guidance Note

IIROC's guidance note, *Frequently Asked Questions – Mandatory Cybersecurity Incident Response*, provides important guidance for compliance with the amended rules, including answers to questions asked in comments on the proposed amended rules. Following is a summary of some important aspects of the guidance.

- **Assessment:** A dealer must use judgment when assessing whether an incident qualifies as a reportable cybersecurity incident, including whether the incident has resulted in, or is likely to result in, "substantial harm" to a person (including individual or entity) or a "material" impact on the dealer's normal operations. The probability of substantial harm may include harm to a non-individual client and may relate to more than just the misuse of personal information. Materiality will vary between dealers of different sizes and business models. A dealer that is uncertain whether an incident constitutes a reportable cybersecurity incident should contact its IIROC relationship manager for guidance.
- **Initial Reports:** The initial report of a cybersecurity incident is meant to reflect only a preliminary assessment, or "brief snapshot of core information," of the incident. IIROC recognizes that a dealer might not have a complete analysis of an incident within three days of discovering it, and expects a dealer to submit the best information available to the dealer at the time of reporting. IIROC also expects a dealer to share with IIROC any additional information the dealer has about an incident.
- **Comprehensive Reports:** The comprehensive report of a cybersecurity incident should include (in addition to the information specified in the rules) all relevant and pertinent information regarding the nature, extent, scope, impact and root cause of the incident, and the actions taken by the dealer to recover, respond and remediate the incident.
- **Time for Filing Comprehensive Report:** If a dealer needs more than 30 days to deliver its comprehensive investigation report, the dealer may request an extension from IIROC. The request should indicate: (1) why the dealer needs more time; (2) when the dealer expects the report to be completed; and (3) when the dealer will submit the report. Dealers that have been granted extensions should keep IIROC informed about the status of the dealer's investigation of the incident and the actions taken by the dealer.
- **False Alarms:** A dealer who submits an initial report of an incident is not required to submit a comprehensive report if the dealer subsequently determines that the incident does not constitute a reportable cybersecurity incident. IIROC strongly recommends that dealers make that determination after consultation with external legal counsel and cybersecurity professionals.
- **IT Service Providers:** The mere fact that a cybersecurity incident takes place at a dealer's service provider does not exclude the incident from the dealer's reporting obligations. A dealer's "information system" or "information stored on such information system," as those terms are used in the rules, include elements supplied by third-party service providers.
- **External Forensic Auditors:** IIROC recommends dealers use an external forensic auditor to investigate a cybersecurity incident, and identify its root cause, if the dealer lacks the specialized knowledge, tools and resources needed to fully investigate the incident, and seeks to manage potential conflicts of interest.
- **IIROC Use of Reported Information:** IIROC intends to share with its dealer community general information about cybersecurity incidents and anonymized information about reported cybersecurity incidents. That kind of information sharing, which is intended to enable other dealers to understand the nature of the cybersecurity risks they might be facing, is consistent with the federal Privacy Commissioner's recent report about mandatory breach reporting trends, which indicates that attackers often re-use the same attacks against multiple organizations in the same industry. (For more information, see BLG bulletin *Mandatory Breach Reporting: Lessons from Year One*.)

Preparing for Compliance with the IIROC Rules

IIROC's amended rules for mandatory cybersecurity incident reporting are now in force. Dealers should promptly assess their systems, policies and procedures, and their readiness to respond to cybersecurity incidents, to ensure that they will be able to submit timely initial incident reports and comprehensive investigation reports. Following are suggestions as to how dealers can ensure preparedness:

- **Policies/Procedures — Assessment and Response:** A dealer should have written policies and procedures so that each potential cybersecurity incident is immediately escalated to designated and properly trained personnel for investigation, assessment and response in accordance with a written incident response plan. This response plan should be consistent with applicable legal requirements, regulatory guidance and relevant best practices. For more information, see BLG bulletins *Cyber Incident Response Plans — Test, Train and Exercise* and *Data Security Incident Response Plans — Some Practical Suggestions*.

- **Policies/Procedures — Reporting to IIROC:** A dealer should have written policies and procedures so that designated and trained personnel make and document informed decisions about reporting cybersecurity incidents to IIROC.
- **Contracts with Data Processors:** A dealer should ensure that its contracts with information technology and data processing service providers (including cloud service providers) contain appropriate provisions (including obligations to promptly notify the dealer of all cybersecurity incidents and provide information about each incident) so that the dealer is able to comply with its cybersecurity incident reporting obligations.
- **Legal Privilege:** A dealer should have an appropriate legal privilege strategy to help avoid inadvertent and unnecessary disclosures of privileged legal advice regarding cybersecurity incidents or inadvertent waivers of legal privilege. For more information, see BLG bulletins *Cyber Risk Management — Legal Privilege Strategy (Part 1)*, *Cyber Risk Management — Legal Privilege Strategy (Part 2)*, *Legal Privilege for Data Security Incident Investigation Reports*, and *Loss of Legal Privilege over Cyberattack Investigation Report*.
- **Other Breach Reporting Obligations:** A dealer should be mindful of its other legal obligations to report, notify and disclose cybersecurity incidents and data security incidents imposed by statute (including personal information protection laws), contract and common law and civil law. For more information, see BLG bulletins *Cyber-Risk Management — Data Incident Notification Obligations*, *Cyber Risk Management — Regulatory Guidance for Reporting Issuers' Continuous Disclosure of Cybersecurity Risks and Incidents*, *Frequently Asked Questions — Compliance with PIPEDA's Security Breach Obligations,* and *OSFI Issues Advisory on Technology and Cybersecurity Incident Reporting*. ■

Authors

Bradley J. Freedman
T 604.640.4129
bfreedman@blg.com

Lauren Phizicky
T 514.395.3889
lphizicky@blg.com

BLG's Cybersecurity Law Group assists clients with legal advice to help manage cyber risks and to respond to data security incidents. Information about BLG's Cybersecurity Law Group is available at **blg.com/cybersecurity**.

BLG Cybersecurity Group – Key Contacts

Bradley J. Freedman	Vancouver	604.640.4129
Éloïse Gratton	Montréal	514.954.3106
Kevin L. LaRoche	Ottawa	613.787.3516
David Madsen	Calgary	403.232.9612
Ira Nishisato	Toronto	416.367.6349