APRIL 2018

CYBERSECURITY BULLETIN

Borden Ladner Gervais

Canadian Investment Industry Regulator Proposes Mandatory Cybersecurity Incident Reporting

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 on April 5, 2018 a notice of proposed amendments to IIROC rules to require IIROC dealer members to report cybersecurity incidents. The reporting obligations apply in a wider range of circumstances than similar reporting obligations under Canadian personal information protection laws. IIROC dealer members should assess their readiness to comply with the reporting obligations, and make appropriate changes to their systems, policies and procedures.

Previous Cybersecurity Guidance

Over the past few years, Canadian investment industry regulators have emphasized the importance of cybersecurity, and have issued guidance to help investment industry participants 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*.

For more information, see BLG bulletins *Cybersecurity Guidance from Investment Industry Organization* (January 2016), *Cybersecurity Guidance from Investment Industry Organization* (May 2016), and *Cybersecurity Guidance from Canadian Securities Administrators*.

IIROC's Proposed Amendments

Details

The proposed amendments broadly define "cybersecurity incident", and require IIROC dealer members to deliver promptly both an initial report and a subsequent detailed investigation report for each cybersecurity incident.

- **Cybersecurity Incident:** The proposed amendments 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: (i) substantial harm or inconvenience to any person (which includes a natural person or legal entity), (ii) a material impact on any part of the dealer's normal operations, (iii) invoking the dealer's business continuity plan or disaster recovery plan, or (iv) 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 proposed amendments 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: (i) a description of the cybersecurity incident, (ii) the date or period during which the cybersecurity incident occurred and the date it was discovered by the dealer, (iii) a preliminary assessment of the cybersecurity incident, including the risk of harm or inconvenience to any person and impact on the operations of the dealer, (iv) a description of immediate incident response steps the dealer has taken to mitigate the risk of harm or inconvenience to persons and the impact on the dealer's operations, and (v) the name of and contact information for an individual who can answer IIROC's follow-up questions.

- **Comprehensive Investigation Report:** The proposed amendments 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: (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 or inconvenienced and the impact on the dealer's operations, (iii) details of the steps the dealer took to mitigate the risk of harm or inconvenience to persons and impact on the dealer's operations, (iv) details of the steps the dealer took to remediate any harm or inconvenience to any persons, and (v) actions the dealer has or will take to improve its cybersecurity incident preparedness.

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

The proposed amendments are open for public comment until May 22, 2018.

IIROC's Explanatory Comments

IIROC's notice provides the following explanatory comments about the proposed amendments:

- Cybersecurity incidents are increasing in frequency and sophistication resulting in increased risk of harm to investors, market participants and dealers.
- The active management of cyber risk is critical to the stability of dealers, the integrity of capital markets and the protection of investors.
- Information sharing is an essential tool for mitigating cyber threats, particularly in a rapidly evolving threat landscape.
- The purpose of the amendments is to "foster fair, equitable and ethical business standards and practices", "promote the protection of investors" and "mitigate a substantial risk of material harm to investors, market participants and [dealers]".
- Prompt cybersecurity incident reporting will help IIROC provide 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.
- A 30-day period after an incident is discovered should provide adequate time for a dealer to complete an incident investigation.
- The proposed amendments are consistent with similar reporting obligations under Canada's *Personal Information Protection and Electronic Documents Act* (PIPEDA), Alberta's *Personal Information Protection Act*, and the New York State Department of Financial Services *Cybersecurity Regulation*.

Uncertainties and Compliance Challenges

IIROC's proposed amendments present some uncertainties and compliance challenges. For example:

- **Substantial Harm/Inconvenience:** When and how should a dealer assess whether a cybersecurity incident has resulted in, or has "a reasonable likelihood" of resulting in, "substantial harm or inconvenience" to an individual or legal entity? What is the intended difference between IIROC's proposed "reasonable likelihood … of substantial harm or inconvenience" test and the "real risk of significant harm" test that applies to PIPEDA's data security incident reporting obligations?
- **Incident Discovery:** When will a dealer be considered to have "discovered" a cybersecurity incident?
- **Reporting:** In what circumstances may a dealer delay reporting a cybersecurity incident, or omit information from a report? For example, may a dealer submit a delayed or modified report to avoid compromising an incident investigation, at the request of law enforcement, to protect commercially sensitive information or to comply with confidentiality obligations?
- **Extensions:** In what circumstances will IIROC agree to extend the 30-day period for delivery of an investigation report?

The notice does not indicate whether IIROC will issue any guidance for compliance with the reporting obligations.

Preparing for Compliance

IIROC's proposed amendments are generally consistent with breach reporting obligations under Canadian personal information protection laws, but would apply in a wider range of circumstances due to the proposed definition of "cybersecurity incident", which is much broader than the kinds of incidents that require reporting under personal information protection laws. For example, IIROC's proposed amendments would appear to require a dealer to report a cybersecurity incident that was effectively mitigated by the dealer's business continuity plan and did not present any risk of harm to the dealer or any other person.

IIROC's proposed amendments do not indicate when they will come into force, and there is no indication that there will be any delay period to allow dealers to prepare for compliance. Accordingly, dealers should now begin assessing and improving their systems, policies and procedures, and designating and training required personnel (both internal employees and external advisors), so that dealers are able to timely submit initial incident reports and comprehensive investigation reports. Following are some suggestions:

- **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 that is 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.
- **Legal Privilege:** A dealer should have an appropriate legal privilege strategy to help avoid inadvertent and unnecessary disclosure of privileged legal advice regarding cybersecurity incidents or inadvertent waiver 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)* and *Legal Privilege for Data Security Incident Investigation Reports*.
- **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 so that the dealer is able to comply with its cybersecurity incident reporting obligations.
- **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*, and *Preparing for Compliance with Canadian Personal Information Security Breach Obligations*. ■

Author

Bradley J. Freedman
T 604.640.4129
bfreedman@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

BLG Vancouver
1200 Waterfront Centre, 200 Burrard St
Vancouver, BC, Canada V7X 1T2
T 604.687.5744 | F 604.687.1415
blg.com