FTR Now

IIROC-Regulated Employers Now Subject to New Cybersecurity Incident Reporting Obligations

Date: November 27, 2019

As of November 14, 2019, investment dealers engaged in trading activity in Canadian markets (Dealer Members) that are regulated by the Investment Industry Regulatory Organization of Canada (IIROC) are now subject to new stringent reporting obligations for cybersecurity incidents. These new rules are the result of amendments to Rules 3100 and 3703 of the IIROC Rules that apply to all Dealer Members.

What is a reportable cybersecurity incident?

Under the IIROC Rules, a “cybersecurity incident” includes any act to gain unauthorized access to, disrupt or misuse the information system of a Dealer Member, or information stored on an information system, that has resulted in or has a reasonable likelihood of resulting in:

1. substantial harm to any person
2. a material impact on any part of the normal operations of the Dealer Member
3. invoking the Dealer Member’s business continuity plan or disaster recovery plan, or
4. the Dealer Member being required under any applicable laws to provide notice to any government body, securities regulatory authority or other self-regulatory organization. (Rule 3100, I.B.1.1 (1); Rule 3703)

What are the new mandatory breach reporting timelines?

The new rules have two reporting requirements:

- within 3 calendar days of discovering a reportable “cybersecurity incident” an Initial Report must be submitted to IIROC
- within 30 days of discovering the incident, or within an extended time period agreed to by IIROC, a Comprehensive Investigation Report must be submitted to IIROC.

What are the reporting obligations?

The Initial 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
3. a preliminary assessment of the cybersecurity incident, including the risk of harm to any person and impact on the operations of the organization
4. a description of immediate steps taken to mitigate the risk of harm to persons and the impact on operations, and
5. a designated contact person who can answer follow-up inquiries. (Rule 3100, I.B.1.1 (3); Rule 3703)

The Comprehensive Investigation 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 Member's operations
3. details of the steps the Dealer Member took to mitigate the risk of harm to persons and the impact on the Dealer Member's operations
4. details of the steps the Dealer Member took to remediate any harm to any persons, and
5. actions the Dealer Member has or will take to improve its cybersecurity incident preparedness. (Rule 3100, I.B. 1.1 (4), Rule 3703)

Concurrent reporting obligations

These new reporting obligations apply in addition to other reporting obligations to which Dealer Members might also be subject. For example, the Office of the Superintendent of Financial Institutions Canada (OSFI) also requires federally-regulated financial institutions to report "high or critical severity" technology and cybersecurity incidents within 72 hours.

The requirement under the IIROC Rules that a cybersecurity incident be reported if a concurrent reporting obligation is triggered highlights the need for financial services organizations to be aware of the myriad of cybersecurity incident reporting obligations that can arise from a single incident.

Put Hicks Morley's experience to work for you

Hicks Morley acts as the regular information, data security and privacy counsel to many private and public sector organizations and understands the myriad of cybersecurity reporting regulations at play. If you would like to discuss cybersecurity preparedness or need help with a ransomware or other data security incidents, please contact your regular Hicks Morley lawyer.