Bulletin | Cybersecurity, Privacy and Data Protection

October 2022

Cybersecurity framework and incident reporting for Ontario's mortgage brokering sector

In August 2022, the Ontario Financial Services Regulatory Authority (FSRA) issued Guidance announcing: (1) FSRA's adoption of the *Principles for Cybersecurity Preparedness for the Mortgage Brokering Sector* (the "Cybersecurity Principles") issued by the Mortgage Broker Regulators' Council of Canada (MBRCC); and (2) a new requirement for mortgage brokerages and administrators to notify FSRA if they experience a cybersecurity incident that could have a material impact on client information. While the Guidance applies to FSRA-regulated mortgage agents, brokers, brokerages and administrators, the Cybersecurity Principles are useful for organizations in all industries.

FSRA Guidance no. MB0048INF

The Guidance explains that the FSRA's adoption of the Cybersecurity Principles is intended to help mortgage agents, brokers, brokerages and administrators in Ontario comply with the *Personal Information Protection and Electronic Documents Act* (concerning the security of personal information) and the *MBRCC Code of Conduct for the Mortgage Brokering Sector* (concerning the security of clients' information) "by providing leading practices for preventing cyber incidents and appropriately responding to them when they occur". FSRA notes that the Cybersecurity Principles take a principles-based approach, which enables regulated persons and entities to achieve specified outcomes in a manner that is "suitable to the size and structure of their business".

The Guidance requires mortgage brokerages and administrators to notify FSRA as soon as they determine that a cybersecurity incident could have a "material impact on client information". The Guidance provides a list of "indicators" that a cybersecurity incident could materially impact clients. The Guidance explains that when FSRA becomes aware of a cybersecurity incident, it will activate its Market Conduct Protocol for Cybersecurity, which outlines FSRA's expected activities with a licensee to monitor the licensee's investigation and response to a cybersecurity incident.

MBRCC Cybersecurity Principles

MBRCC is a forum for Canadian mortgage broker regulators to collaborate and promote greater regulatory consistency to serve the public interest. MBRCC published the Cybersecurity Principles to support cybersecurity preparedness in the mortgage brokering sector by describing practices to avoid cybersecurity incidents and properly respond to them when they occur.

The Cybersecurity Principles are intended to align with existing legal requirements, including professional-client confidentiality obligations and privacy obligations under personal information protection laws. The Cybersecurity Principles are based on recognized best practices, including the NIST Cybersecurity Framework and OSFI's Guideline B-13 – Technology and Cyber Risk Management.

The Cybersecurity Principles articulate four principles, supported by specific recommended actions, that describe desired outcomes for cybersecurity preparedness. Following is a summary:

- **Responsibility and resourcing:** Regulated entities should appoint a person responsible for overseeing cybersecurity risk, and invest and assign all resources needed to develop and maintain effective cybersecurity safeguards to protect client information. Regulated entities should develop cybersecurity preparedness policies and procedures, require responsible individuals to maintain their skillset and understanding of cybersecurity risks through ongoing education, raise staff and management awareness of cybersecurity risks to ensure cybersecurity preparedness, and consider purchasing cybersecurity liability insurance.
- **Identification and prevention of risks:** Regulated entities should identify key cybersecurity risks, have appropriate "endpoint" risk detection protections, conduct a cyber incident business impact assessment and ensure cybersecurity risks are part of the business continuity plan, take adequate steps to minimize the likelihood and impact of a risk once identified, and determine the entity's comfort with identified risks.
- **Incident monitoring, detection and response:** Regulated entities should have a protocol for monitoring, detecting and responding to cybersecurity incidents, and an incident response plan to protect client information and minimize service disruptions if an incident is detected.
- **Third-party management:** Regulated entities should protect clients' information by taking reasonable steps to ensure that their external third-party services providers have established cybersecurity preparedness practices.

The Cybersecurity Principles include a basic cybersecurity preparedness checklist for use by regulators to evaluate cybersecurity preparedness as part of their monitoring programs and by regulated entities to self-assess their cybersecurity preparedness.

Comments and recommendations

- **Three pillars:** The Cybersecurity Principles reflect the view that effective technology and cyber risk management is an enterprise-wide risk management and compliance challenge that requires a comprehensive, multidisciplinary approach based on three pillars – people, processes and technology.
- **Continuous improvement:** Compliance with the Cybersecurity Principles is not a one-time event. The Cybersecurity Principles require regulated entities to establish processes and procedures to continuously monitor and improve their cybersecurity posture.
- **Other Guidance:** When preparing for compliance with the Cybersecurity Principles, regulated entities should consider similar guidance and best practices recommended by Canadian government agencies, regulators, privacy commissioners, industry associations and other organizations, such as the British Columbia Financial Services Authority's Outsourcing Guideline and Information Security Guideline. See BLG bulletin *BCFSA finalizes information security and outsourcing guidelines*.
- **Other legal requirements:** When preparing for compliance with the Cybersecurity Principles, regulated entities should be mindful of other restrictions and requirements, imposed by privacy/personal information protection laws and contracts, regarding the handling of personal information.
- **Directors and officers:** A regulated entity's directors and senior officers should have direct involvement in the entity's compliance with the Cybersecurity Principles. Their decisions should be made with documented due care (i.e., based on accurate information and expert advice) to achieve the best outcome and support the application of the "business judgment rule". See BLG bulletin *Cyber risk management guidance for Canadian corporate directors*.

- **Legal privilege:** Compliance with the Cybersecurity Principles and other risk management activities may result in sensitive communications and documents that might be subject to mandatory disclosure in regulatory investigations and legal proceedings unless the communications and documents are protected by legal privilege. Where appropriate, regulated entities should take steps to establish and maintain legal privilege over communications and documents relating to compliance with the Cybersecurity Principles. See BLG bulletins *Cyber Risk Management – Legal Privilege Strategy – Part 1* and *Cyber Risk Management – Legal Privilege Strategy – Part 2*.
- **Risk-based decisions:** Compliance with the Cybersecurity Principles will require regulated entities to make numerous risk-based decisions to achieve specified outcomes "in a manner that is suitable for the size and structure of their business". Each of those decisions should be fully informed (based on timely, complete and reliable information), made with the benefit of appropriate advice from independent technical experts and legal counsel, and properly documented. ■

Authors

Bradley J. Freedman
T 604.640.4129
bfreedman@blg.com

Donna Spagnolo
T 416.367.6236
dspagnolo@blg.com

BLG's Cybersecurity, Privacy & Data Protection Group has extensive expertise and experience providing cyber risk management and incident response legal services to regulated financial institutions. Find out more at **blg.com/cybersecurity**.