FSRA
Financial Services Regulatory Authority of Ontario

Information

Effective Date: August 18, 2022
Identifier: No. MB0048INF

Mortgage Broker Regulators' Council of Canada Principles for Cybersecurity Preparedness for the Mortgage Brokering Sector

Purpose

This guidance provides Information on FSRA's:

- adoption of the Mortgage Broker Regulators' Council of Canada's Principles for Cybersecurity Preparedness for the Mortgage Brokering Sector ("MBRCC Cybersecurity Guidance") into FSRA's regulatory framework
- "Market Conduct Protocol for Cybersecurity" which is activated for engagement with licensees that experience a cybersecurity incident that could have a material impact on client information

The MBRCC Cybersecurity Guidance was developed to help enhance cybersecurity preparedness within the mortgage brokering sector through the creation of suggested leading practices for preventing cybersecurity incidents and appropriately responding to them when they occur.

Scope

This guidance affects the following individuals and entities regulated by FSRA:

- mortgage agents
- mortgage brokers
- mortgage brokerages
- mortgage administrators

Rationale and background

Cyberattacks represent a significant risk in the sectors which FSRA regulates. The flow of information between mortgage brokerages, administrators, lenders / investors, borrowers, and third-party service providers is vulnerable to interference or being compromised.

Cybersecurity is the application of technologies, processes and controls to protect infrastructure such as systems, networks, programs, devices and data. It aims to reduce the likelihood and impact of cyberattacks which could result in unauthorized access to sensitive client information and disruption of business activities due to interference with critical infrastructure and corporate networks.

For some entities, cybersecurity risk management should be a component of Information Technology (IT) risk management policies and procedures, targeted to mitigate internal and external threats to their IT systems, infrastructure and data.

The MBRCC Cybersecurity Guidance, and FSRA's adoption of the guidance, is intended to support cybersecurity preparedness within the mortgage brokering sector by providing leading practices for preventing cyber incidents and appropriately responding to them when they occur.

As a Market Conduct regulator FSRA's goal is to protect unauthorized access to sensitive client information. For the purposes of this guidance client information refers to all consumer information, including for borrowers, lenders / investors, and prospective clients.

FSRA mandate

In supervising and regulating the mortgage brokering sector, FSRA aims to achieve its statutory objects, which for the purposes of informing this Guidance, include:

- contribute to public confidence in the mortgage brokering sector
- monitor and evaluate trends in the mortgage brokering sector
- cooperate and collaborate with other regulators where appropriate
- protect the rights and interests of consumers

Information

Legal framework for personal information

The Canadian legal framework requires the protection of personal information. Under the federal *Personal Information Protection and Electronic Documents Act* and the proposed federal *Consumer Privacy Protection Act*, all businesses, including mortgage brokerages and administrators, have obligations to protect specific personal client information. For example, personal data collected must be maintained securely and protected from personal loss, unauthorized access, and data theft.

MBRCC Code of Conduct for the Mortgage Brokering Sector

Under Principle 8 of the MBRCC Code of Conduct for the Mortgage Brokering Sector, “regulated persons and entities must protect their clients’ information. They must use and disclose it only for purposes for which the client has given consent or as compelled by law.”

MBRCC cybersecurity guidance

To support FSRA licensed entities with these obligations and to effectively manage cybersecurity risks, FSRA expects entities to implement the “Principles” identified in the MBRCC Cybersecurity Guidance. The Principles describe the outcomes that regulated entities should achieve to ensure cybersecurity preparedness, without prescribing how they should be achieved. This principles-based approach enables regulated entities to achieve the outcomes in a manner that is suitable to the size and structure of their business.

The MBRCC Cybersecurity Guidance includes a checklist to help entities self-assess their cybersecurity preparedness.

Continuing education requirement

Under section 9 of Ontario Regulation 409/07 (O. Reg. 409/07) under the *Mortgage Brokerages Lenders, and Administrators Act (2006),* FSRA has the authority to establish continuing education (CE) requirements for mortgage agents and brokers. Agents and brokers seeking to renew a licence must successfully complete the CE requirement approved by the Chief Executive Officer (CEO) of FSRA.

FSRA's CE requirements include cybersecurity education/topics, as needed. The objective of this CE is to ensure that each licensee understands how to identify and take action to protect against cybersecurity threats. For mortgage brokerage and administrator operations, FSRA wants to support industry in ensuring processes are in place to identify, monitor and respond to cybersecurity risks, to help ensure the protection of client information.

FSRA's Market Conduct Protocol for Cybersecurity

Notification of cybersecurity incidents

Mortgage brokerages and administrators should notify[1] FSRA by e-mailing the 'IT Risk Incident Notification Form' to ITriskinbox@fsrao.ca or uploading it and any other supporting documentation to the Incident Notification Portal if they experience a cybersecurity incident that could have a material impact on client information.

FSRA wants to ensure:

- appropriate steps are taken to protect clients
- the regulator has up to date information to address any public inquiries
- there is consistent messaging by the regulator and the licensee to prevent undue alarm

Notification to the regulator should occur as soon as a licensee determines a cybersecurity incident could have a material impact on clients. The following are indicators that a cybersecurity incident could have a material impact on clients:

[1] Previously, notification to FSRA of cybersecurity incidents was by e-mail at MBconduct@fsrao.ca

- the security breach impacted a system or database that stores a large amount or a sizable proportion of sensitive client information
- if the mortgage brokerage or administrator would, in the normal course of operations, escalate the matter to or inform senior management accountable for information security
- the security incident requires non-routine measures or resources by the mortgage brokerage or mortgage administrator
- the security incident has resulted in a cyber insurance claim being initiated
- the breach is a repeat incident and could have a material impact on a cumulative basis

Activation of FSRA's Market Conduct Protocol for Cybersecurity

When FSRA becomes aware of a cybersecurity incident through notification by a licensee, market intelligence, a tip or complaint, it will activate *FSRA's Market Conduct Protocol for Cybersecurity*.

The protocol outlines FSRA expected engagement with the licensee[2] to monitor the entity's actions in investigating and responding to the incident. The engagement is continuous, until FSRA has:

- a complete understanding and knowledge of the extent of the potential data breach and what information was accessed
- confirmation that any corrupted information has been restored and/or that the breach has been mitigated or contained
- confirmation that all systems are back online and fully functional
- confirmation that all affected stakeholders, including clients and relevant privacy regulators, have been notified, and reasonable steps have been taken by the licensee to limit potential client harm
- a complete understanding and knowledge of the safeguards that have been put in place to ensure the licensee is protected from similar future breaches

FSRA will maintain confidentiality of incidents reported to the extent allowed by the law.

[2] Should FSRA require additional information regarding an incident, per s. 29 of the MBLAA, FSRA has authority to require licensees to give the CEO additional information and documents as the CEO may request, and to do so in the manner and within the period specified by the CEO.

Incident response typically proceeds in phases similar to the pattern below:

Phase 1: Receive immediate information from the licensee about what they know about the nature and extent of the cybersecurity incident, what they have done to recover and respond, and what additional actions are planned.

Phase 2: As more complete information becomes available, receive regular updates from the licensee on the extent/impact of the incident on its clients and services. Information requested depends on the nature of the incident. For example, in the case of a data breach, FSRA will seek a clear understanding of the nature and extent of the data breach and the risks it presents to client information.

Phase 3: FSRA receives the licensee's plan to prevent a similar cybersecurity incident in the future.

FSRA's level / frequency of engagement with a licensee reflects the nature and impact of the cybersecurity incident and will consider resources required of the licensee to respond to the incident.

Effective date and future review

This guidance is effective August 18, 2022 and will be reviewed no later than August 18, 2025.

About this guidance

This document is consistent with FSRA's Guidance Framework. As Information guidance, it describes FSRA's views on certain topics without creating new compliance obligations for regulated persons.

References

- MBRCC Principles for Cybersecurity Preparedness
- MBRCC Code of Conduct
- FSRA Information Technology Risk Management Guidance[3]

Effective Date: August 18, 2022

Last Updated: April 12, 2024

[3] FSRA IT Risk Management Guidance published April 1, 2024