NEW COMPLIANCE REQUIREMENTS FOR QUÉBEC FINANCIAL INSTITUTIONS: OVERVIEW OF THE *REGULATION RESPECTING THE MANAGEMENT AND REPORTING OF INFORMATION SECURITY INCIDENTS BY CERTAIN FINANCIAL INSTITUTIONS AND BY CREDIT ASSESSMENT AGENTS*

Posted on January 15, 2025

Categories: Insights, Publications

On October 23, 2024, the Québec government published the *Regulation respecting the management and reporting of information security incidents by certain financial institutions and by credit assessment agents* (the "**Regulation**") in the *Gazette officielle du Québec*. The obligations set out in the Regulation will come into force on April 23, 2025.

Broadly, the Regulation establishes three key set of obligations on Financial Institutions, namely (i) an information security incident management policy, (ii) information security incident reporting obligations, and (iii) information security incident record-keeping requirements.

This bulletin provides an overview of the Regulation's key obligations affecting Financial Institutions.

A. Affected Organizations

The Regulation applies to the following financial institutions ("**Financial Institutions**"):

- insurers authorized under the *Insurers Act* and federations of mutual companies that are subject thereto,
- federations and credit unions not members of a federation that are subject to the *Act respecting financial services cooperatives*,
- deposit institutions authorized under the Deposit Institutions and Deposit Protection Act,
- trust companies authorized under the *Trust Companies and Savings Companies Act*, and
- credit assessment agents designated under the *Credit Assessment Agents Act*.

B. Scope of the Regulation

The Regulation defines a "information security incident" as an attack on the availability, integrity or

confidentiality of information systems or the information they contain.

This definition is to be contrasted with a "confidentiality incident," as defined in the *Act respecting the protection of personal information in the private sector* ("**Private Sector Act**") applicable to private-sector organizations as (1) access not authorized by law to personal information; (2) use not authorized by law of personal information; (3) communication not authorized by law of personal information; or (4) loss of personal information or any other breach of the protection of such information.[1]

While the Private Sector Act refers to unauthorized access, use, communication, or loss of personal information, the Regulation refers to an "attack" on the "availability," "integrity," or "confidentiality" of "information systems" and the "information" they contain. As a result, the Regulation may apply to attacks on information systems and also on any information held by a Financial Institution, including personal information.

C. Information Security Incident Management Policy

An important obligation imposed on affected institutions is to develop, implement and maintain an information security incident management policy. Such policy must include procedures and mechanisms for detecting, assessing and responding to information security incidents that may occur within the Financial Institution, a procedure for reporting information security incidents to officers or managers, where applicable (the "**Officers**"), and a procedure for reporting information security incidents to other stakeholders, including its clients, third parties to which the Financial Institution has entrusted the performance of any part of its activities, consumers, the *Autorité des marchés financiers* ("**AMF**"), and any other regulatory bodies.

Pursuant to the Regulation, Financial institutions must formally assign, in writing, the responsibility for overseeing the management and reporting of information security incidents to one of its Officers.

D. Reporting Obligations

The Regulation also imposes various reporting obligations on Financial Institutions.

i. Potential Adverse Impacts and Crime Prevention

In the event of an information security incident having potential adverse impacts is reported to the Officer, the Financial Institution must notify the AMF of the incident within twenty-four hours of receiving the report information security incident. The Officer must also notify the AMF, within the same delay, of any information security incident subject to a notice to a regulatory body or a person or entity responsible under the law for the prevention, detection, repression of crime or statutory offences or contractually responsible for providing compensation for injuries arising from such incident.

ii. Reports to the Commission *d'accès à l'information*

If a Financial Institution has cause to believe that a confidentiality incident involving personal information has occurred and presents a "risk of serious injury" to the individuals concerned under the Private Sector Act, the Financial Institution must not only notify the *Commission d'accès à l'information du Québec* ("**CAI**") as required by the Private Sector Act but also, under the Regulation, must notify the AMF at the same time.

iii. Ongoing Reporting Obligations

Once a notice of an information security incident is given by the Financial Institution to the AMF under the Regulation, the Financial Institutions must continue notifying the AMF of any developments in the situation every three days thereafter and continue providing updates to the AMF every three days until the Financial Institution is able to confirm to the AMF that incident is brought under control and that operations have returned to normal.

Then, within thirty days following the confirmation that the incident has been brought under control and that operations have returned to normal, the Financial Institution must send the AMF a report mandatorily covering the following:

- the identification of the source and type of the information security incident;
- the Financial Institution's assessment regarding the potential recurrence of the incident; and
- a description of the actions taken by the Financial Institution to reduce the likelihood of incidents of a similar nature occurring in the future.

iv. Information Security Incident Register

The Regulation mandates Financial Institutions to maintain a current information security incident register that must include the following for each incident:

- the date, time and location of the incident,
- the nature of the incident,
- a detailed description of the incident,
- any injury caused by the incident,
- any third parties involved,
- any actions taken,
- whether the residual risk is accepted or not accepted and the rationale behind it,
- any planned actions, and
- the incident close date.

The Regulation also requires Financial Institutions to keep the information recorded in the register secure and

confidential so as to maintain the integrity of the information for at least five years from the date of its detailed report provided to the AMF under the Regulation.

E. Monetary Administrative Penalties

The Regulation provides for administrative penalties in the event Financial Institutions fail to comply with their obligations.

More specifically, Financial Institutions may be penalized for failing to (i) assign responsibility for monitoring the management and reporting of information security incidents, (ii) notify the AMF of an information security incident within required timeframes, (iii) fails to notify the AMF in instances when it was required to notify the CAI, (iv) or provide necessary ongoing reports on incidents. These penalties can range from $250 for individuals to $1,000 for Financial Institutions.

Financial Institutions can also be subject to higher administrative penalties for failing to (i) develop or implement the required policy, (ii) maintain current its information security incident register, or (iii) keep the information in the register for at least five years as required by the Regulation. Such penalties can range from $500 for individuals to $2,500 for Financial Institutions.

F. Takeaways

The Regulation implements more stringent requirements on Financial Institutions with respect to the management and reporting of information security incidents. Going forward, Financial Institutions should not only comply with the obligations set out in the Regulation but also be mindful of their reporting obligations across various regulatory frameworks.

For a detailed analysis of how the Regulation may affect your operations, or to obtain further information and assistance with implementing and maintaining your information security incident management policy and procedures, please contact McMillan LLP's Privacy & Data Protection Group. We are committed to providing you with tailored advice that ensures your data protection strategies are both compliant and effective in Quebec's complex regulatory landscape.

[1] Section 3.6, *Act respecting the protection of personal information in the private sector*, CQLR c P-39.1.

by Amir Kashdaran, Mitch Koczerginski, and Meena Shanmuganathan (Articling Student)

A Cautionary Note