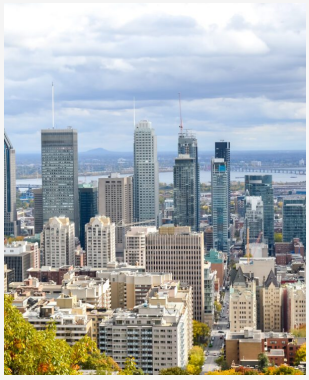
OSLER

The Québec AMF's new information security incident reporting regime: what financial institutions need to know

DECEMBER 3, 2024 8 MIN READ



Related Expertise

- Cybersecurity and Security Incident Response
- Financial Services
- Financial Services Regulatory
- Privacy and Data Management

Authors: Éloïse Gratton, Ad. E., François Joli-Coeur, Justin P'ng, CIPP/C/US, Marguerite Rolland

On October 23, 2024, Québec's Autorité des marchés financiers (AMF) published the *Regulation respecting the management and reporting of information security incidents by certain financial institutions and by credit assessment agents* [PDF] (AMF Regulation). Effective April 23, 2025, information security incident management and disclosure obligations for certain financial institutions and credit assessment agents will come into force. We note that many of these requirements align with expectations outlined in the AMF's Guideline on Information and Communications Technology Risk Management.

This article outlines the key obligations of the AMF Regulation and compares them with two existing reporting frameworks: the Office of the Superintendent of Financial Institutions's (OSFI) Technology and Cyber Security Incident Reporting Advisory (OSFI Advisory) and the *Regulation respecting confidentiality incidents* (Private Sector Regulation) under Québec's *Act respecting the protection of personal information in the private sector* (ARPPIPS).

Scope

The AMF Regulation applies to insurers,[1] federations and credit unions,[2] deposit institutions,[3] trust companies[4] and credit assessment agents[5] operating in Québec (collectively, Financial Institutions). Due to their operations in Québec, such organizations are generally subject to the Private Sector Regulation,[6] and certain of these organizations or their operations are regulated as federally regulated financial institutions (FRFI) subject to the OSFI Advisory. As we discuss below, the entities subject to these other two reporting regimes should be well positioned to comply with the AMF Regulation given its overlap with these existing regimes.

The AMF Regulation specifically applies to "information security incidents," which are defined as "an attack on the availability, integrity or confidentiality of information systems or the information they contain."[7] In comparison, the OSFI Advisory applies to a "technology or cybersecurity incident," which is "an incident that has an impact, or the potential to have an impact on the operations of a FRFI, including its confidentiality, integrity or the availability of its systems and information,"[8] whereas the ARPPIPS more narrowly applies to "confidentiality incidents," which concern the unauthorized use or communication of, loss of,

or other breach of the protection of personal information.[9]

Reporting threshold

Under the AMF Regulation, an information security incident must be reported to the AMF when it has been (1) reported to the officers or managers of the Financial Institution and has "potentially adverse impacts" or (2) reported, in a notice or otherwise, to a regulatory body or to a person or body with either a legal mandate to prevent, detect or repress offences, or a contractual mandate to compensate for injuries resulting from the incident. In addition, a confidentiality incident reported to the Commission d'accès à l'information (CAI) must also be reported to the AMF.[10]

An incident that meets this threshold would likely also meet the threshold under the OSFI Advisory, which defines a reportable incident as one which may meet any one of 16 criteria, including impact to FRFI operations, infrastructure, systems or data.[11] Similarly, the OSFI Advisory includes incidents that are "reported to other local or foreign supervisory or regulatory organizations or agencies" as a trigger for reporting an incident to OSFI.[12] In contrast, the reporting threshold under the ARPPIPS only requires reporting an incident to the CAI where there is a risk of *serious* injury to impacted individuals.[13]

Key obligations

The AMF Regulation specifies several obligations for financial institutions, which we discuss and compare to other reporting frameworks below.

Initial notification to regulator

Under the AMF Regulation, Financial Institutions must report information security incidents to the AMF within 24 hours of reporting the incident internally to the institution's officers or managers or externally per the above criteria.[14] Similarly, under the OSFI Advisory, FRFIs must report a technology or cybersecurity incident to OSFI's Technology Risk Division within 24 hours of the incident (or sooner if possible).[15] Under the Private Sector Regulation, however, confidentiality incidents must be reported "promptly" to the CAI, which may provide more flexibility to organizations.[16]

Notification of developments

The AMF Regulation requires that Financial Institutions update the AMF on incident developments every three days following the initial notification until an incident resolution notice is submitted (other than for confidentiality incidents reported to the CAI).[17] This requirement differs from the OSFI Advisory as OSFI expects FRFIs to provide updates "as information becomes available," with an example cadence of daily updates.[18] The Private Sector Regulation only requires that certain developments be notified to the CAI "promptly."[19]

Form and contents of notification

Per the AMF Regulation, Financial Institutions must report an incident to the AMF by completing a form available on the regulator's website (which is not yet available).[20] The OSFI Advisory also requires that FFRIs report an incident by completing a form [PDF] available on

OSFI's website and transmitting it to OSFI's Technology Risk Division.[21] Broadly, the reporting form under the OSFI Advisory requires that FFRIs provide

1. incident and contact information
2. the site location and lines of business affected
3. a description of the incident and related risks
4. the incident level of priority
5. information about internal and external notifications of the incident[22]

The Private Sector Regulation, meanwhile, requires a notice in writing to the CAI, but does not mandate the use of the form [PDF] made available by the regulator.[23] The notice can be sent by email or regular mail. It requires that the following information be included in an incident notice:

1. the name and Québec business number of the organization and the name and contact information of a representative
2. a description of personal information covered by the incident and of the circumstances and cause of the incident
3. the date or time period when the incident occurred, and when the organization became aware of the incident
4. the number of people the incident concerns and the number of those residing in Québec
5. a description of the organization's evaluation of whether there is a serious risk of injury
6. information related to notifying persons whose personal information the incident concerns
7. the mitigation and risk-reduction measures the organization has taken post-incident or intends to take, including timelines for implementation
8. whether another privacy regulator has been notified of the incident[24]

Final incident report

Within 30 days following a Financial Institution's incident resolution notice to the AMF, the institution must also send the regulator a report that

1. identifies the source and type of incident
2. provides an assessment of recurrence potential
3. describes the measures taken to reduce the risk of future similar incidents[25]

The OSFI Advisory also requires this type of post-incident report, but offers less specificity as the report only requires the FRFI's post-incident review and lessons learned.[26] The Private Sector Regulation and the ARPPIPS do not mandate any post-incident report to the CAI.

Incident register

The AMF Regulation requires that financial institutions maintain an up-to-date information security register containing the following information:

- the date and time of the incident
- the location of the incident

- the nature of the incident
- a detailed description of the incident, including an assessment of a potential recurrence of the incident
- any injury caused by the incident
- any third parties involved in the incident
- actions taken
- whether the residual risk is accepted or not accepted and the rationale for accepting it or not
- planned actions
- the incident close date[27]

The Private Sector Regulation requires a confidentiality incident register with substantively similar contents and some differences.[28] In contrast, the OSFI Advisory does not require that an FRFI maintain an incident register whatsoever, nor does OSFI's Guideline on Technology and Cyber Risk Management recommend it as a best practice.

Information security incident management policy

Under the AMF Regulation, Financial Institutions are required to implement an incident management policy that includes procedures and mechanisms for detecting, assessing and responding to information security incidents, and for reporting such incidents to the officers or managers of the Financial Institution and any other stakeholders (including clients, service providers, consumers, the AMF itself and other regulatory bodies).[29]

The AMF Regulation also requires that responsibility for incident management and reporting be assigned in writing to a designated officer or manager.[30] While the OSFI Advisory lacks obligations regarding incident management policies and the responsibility thereof, the OSFI Guideline on Technology and Cyber Risk Management sets out directly comparable, but optional, recommendations.

While the governance obligations under the Private Sector Regulation and the ARPPIPS are less prescriptive, they still broadly require the establishment and implementation of governance policies and practices which ensure the protection of personal information and require the naming of a privacy officer.[31]

Recommendations and steps to compliance

Depending on which type of Financial Institution a given organization is, the preparation for compliance with the AMF Regulation will differ. In either case, organizations should be mindful that monetary administrative penalties ranging from $250 to $2,500 CAD may be imposed for non-compliance with the AMF Regulation, depending on the type of contravention.[32]

FFRIs already operating in Québec

FRFIs with existing operations in Québec that are already positioned to comply with the OSFI Advisory, the ARRPIPS and the Private Sector Regulation are substantively positioned to comply with the AMF Regulation. Collectively, the other two reporting regimes substantially overlap with the AMF Regulation. However, a review of compliance programs and service provider agreements is advisable to identify and address any gaps in compliance procedures.

Financial institutions not regulated by OSFI

Organizations that are not regulated by OSFI (and thus not subject to the OSFI Advisory) may need to undertake more substantive compliance efforts. While these organizations should already be set up to comply with the Private Sector Regulation due to their operations in Québec, the Private Sector Regulation's requirements are less specific and prescriptive than those contained in the AMF Regulation. Accordingly, these organizations will need to adapt their compliance programs and service provider agreements to reflect the AMF Regulation's requirements.

---

[1] Insurers authorized under the *Insurers Act* and federations of mutual companies that are subject thereto.

[2] Federations and credit unions not members of a federation that are subject to the *Act respecting financial services cooperatives*.

[3] Deposit institutions authorized under the *Deposit Institutions and Deposit Protection Act*.

[4] Trust companies authorized under the *Trust Companies and Savings Companies Act*.

[5] Credit assessment agents designated under the *Credit Assessment Agents Act*.

[6] Private Sector Regulation, article 1.

[7] AMF Regulation, article 2.

[8] OSFI Advisory, "Scope and Definition."

[9] ARPPIPS, article 3.6.

[10] AMF Regulation, articles 5 and 6.

[11] OSFI Advisory, "Criteria for Reporting."

[12] OSFI Advisory, "Criteria for Reporting."

[13] ARPPIPS, articles 3.5, para. 2, 3.7.

[14] AMF Regulation, article 5.

[15] OSFI Advisory, "Initial Notification Requirements."

[16] ARPPIPS, article 3.5, para. 2.

[17] AMF Regulation, article 8.

[18] OSFI Advisory, "Subsequent Reporting Requirements."

[19] AMF Regulation, article 4.

[20] AMF Regulation, article 7.

[21] OSFI Advisory, “Initial Reporting Requirements.”.

[22] See the OSFI Technology and Cyber Incident Report form [PDF].

[23] Private Sector Regulation, article 3.

[24] Private Sector Regulation, article 3.

[25] AMF Regulation, article 9.

[26] OSFI Advisory, “Subsequent Reporting Requirements.”

[27] AMF Regulation, article 10.

[28] Private Sector Regulation, article 7.

[29] AMF Regulation, article 3.

[30] AMF Regulation, article 4.

[31] ARPPIPS, article 3.1, para 2, 3.2.

[32] AMF Regulation, articles 12–13.