REGULATION RESPECTING THE MANAGEMENT AND REPORTING OF INFORMATION SECURITY INCIDENTS BY CERTAIN FINANCIAL INSTITUTIONS AND BY CREDIT ASSESSMENT AGENTS

Credit Assessment Agents Act
(chapter A-8.2, ss. 66 and 73)

Insurers Act
(chapter A-32.1, ss. 485 and 496)

Act respecting financial services cooperatives
(chapter C-67.3, ss. 601.1 and 601.9)

Deposit Institutions and Deposit Protection Act
(chapter I-13.2.2, s. 43, par. *u* and s. 45.9)

Trust Companies and Savings Companies Act
(chapter S-29.02, ss. 277 and 286)

CHAPTER I
SCOPE AND INTERPRETATION

1. This Regulation applies to the following financial institutions:

(1) insurers authorized under the Insurers Act (chapter A-32.1) 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 (chapter C-67.3);

(3) deposit institutions authorized under the Deposit Institutions and Deposit Protection Act (chapter I-13.2.2); and

(4) trust companies authorized under the Trust Companies and Savings Companies Act (chapter S-29.02).

This Regulation also applies to credit assessment agents designated under the Credit Assessment Agents Act (chapter A-8.2).

2. For purposes of this Regulation, “information security incident” means an attack on the availability, integrity or confidentiality of information systems or the information they contain.

CHAPTER II
MANAGEMENT OF INFORMATION SECURITY INCIDENTS

DIVISION I
INFORMATION SECURITY INCIDENT MANAGEMENT POLICY

3. A financial institution or a credit assessment agent must develop and implement an information security incident management policy that includes, without limitation, procedures and mechanisms for detecting, assessing and responding to information security incidents where such incidents occur within the institution, a credit union that is a member of a federation, the agent or a third party to which the institution, the credit union or the agent has entrusted the performance of any part of an activity.

The information security incident management policy must also contain a procedure for the reporting of information security incidents to the officers or, as the case may be, to the managers of the financial institution or the credit assessment agent, including a procedure

for the reporting of such incidents thereto when they occur within a credit union that is a member of a federation or a third party contemplated in paragraph 1.

Furthermore, the policy must include a procedure for the reporting of incidents to any other stakeholders, including clients, third parties to which the institution or agent has entrusted the performance of any part of an activity, consumers, the Autorité des marchés financiers and any other regulatory bodies.

4. A financial institution or a credit assessment must assign, in writing, responsibility for monitoring the management and reporting of information security incidents to one of its officers or, in the case of a financial services cooperative, to one of its managers.

DIVISION II
REPORTING TO THE AUTORITÉ DES MARCHÉS FINANCIERS

5. A financial institution or a credit assessment agent must, if an incident with potentially adverse impacts is reported to its officers or, as the case may be, to its managers, report the incident to the Authority no later than 24 hours after the incident.

The financial institution or the credit assessment agent must, within that same period, also report to the Authority any information security incident that has been reported to a regulatory body, a person or a body responsible under law for the prevention, detection or repression of crime or statutory offences or contractually responsible for providing compensation for injury that may have been caused by the incident.

6. When a financial institution or a credit assessment agent notifies the Commission d'accès à l'information, established under section 103 of the Act respecting Access to documents held by public bodies and the Protection of personal information (chapter A-2.1), of a confidentiality incident referred to in paragraph 2 of section 3.5 of the Act respecting the protection of personal information in the private sector (chapter P-39.1), it must report the incident to the Authority at the same time.

7. A financial institution or a credit assessment agent must report an information security incident to the Authority by completing the form available on the Authority's website.

8. A financial institution or a credit assessment agent must notify the Authority of developments in the situation no later than three days following the notice referred to in section 5 and no later than every three days thereafter, until the close of the incident.

9. Within three days from the close of the incident, a financial institution or a credit assessment agent must send to the Authority a notice confirming that the incident is under control and that operations have returned to normal.

10. A financial institution or a credit assessment agent must send the Authority a report within 30 days from the close of the information security incident. The report must, among other things:

(1) identify the source and type of the incident;

(2) provide an assessment by the financial institution or the credit assessment agent regarding a potential recurrence of the incident; and

(3) describe the actions taken to reduce the possibility of new incidents of the same nature occurring.

DIVISION III
INFORMATION SECURITY INCIDENT REGISTER

11. A financial institution or a credit assessment agent must maintain a current information security incident register that includes, for each incident:

(1) the date and time of the incident;

(2) the location of the incident;

(3) the nature of the incident;

(4) a detailed description of the incident, including the information specified in subparagraph 2 of section 10;

(5) any injury caused by the incident;

(6) the third parties involved in the incident;

(7) the actions taken;

(8) acceptance or non-acceptance of the residual risk and the reasons for such acceptance or non-acceptance;

(9) planned actions; and

(10) the incident close date.

12. A financial institution or a credit assessment agent must keep the information recorded in the register in a secure and confidential manner so as to maintain the information's integrity for a minimum period of seven years from the date of the report referred to in section 10.

CHAPTER III
MONETARY ADMINISTRATIVE PENALTIES

13. A monetary administrative penalty of $250, in the case of a natural person, and $1,000, in any other case, may be imposed on a financial institution or a credit assessment agent contemplated in section 1 that:

(1) in contravention of section 4, has not assigned, in writing, responsibility for monitoring the management and reporting of information security incidents to one of its officers or, as the case may be, to one of its managers;

(2) in contravention of section 5, fails to report an incident to the Authority no later than 24 hours after the incident;

(3) in contravention of section 6, fails, when notifying the Commission d'accès à l'information of an incident, to report the incident to the Authority at the same time;

(4) in contravention of section 8, fails to notify the Authority of developments in the situation no later than three days following the notice referred to in section 7 and no later than every three days thereafter, until the close of the incident; or

(5) in contravention of section 9, fails to send to the Authority, within three days from the close of an information security incident, a notice consistent with this section;

14. A monetary administrative penalty of $500, in the case of a natural person, and $2,500, in any other case, may be imposed on a financial institution or a credit assessment agent referred to in section 1 that:

(1) in contravention of section 3, fails to develop or implement an information security incident management policy;

(2) in contravention of section 11, fails to maintain a current information security incident register; or

(3) in contravention of section 12, fails to keep the information in the information security incident register for a minimum period of seven years from the date of the report contemplated in section 10.

CHAPTER IV
FINAL PROVISION

15. This Regulation comes into force on (*indiquer ici la date d'entrée en vigueur du présent règlement*).