M.O., 2024-13

Order number 2024-13 of the Minister of Finance, 7 October 2024

Credit Assessment Agents Act
(chapter A-8.2)

Insurers Act
(chapter A-32.1)

Act respecting financial services cooperatives
(chapter C-67.3)

Deposit Institutions and Deposit Protection Act
(chapter I-13.2.2)

Trust Companies and Savings Companies Act
(chapter S-29.02)

CONCERNING the Regulation respecting the management and reporting of information security incidents by certain financial institutions and by credit assessment agents

WHEREAS section 66 of the Credit Assessment Agents Act (chapter A-8.2) stipulates that, in addition to the other regulations it may make under this Act, the *Autorité des marches financiers* may, by regulation, determine the standards that apply to credit assessment agents as regards their commercial practices and management practices;

WHEREAS the first paragraph of section 67 of the said Act stipulates that a regulation made under this Act by the *Autorité des marches financiers* is approved by the Minister of Finance with or without amendment;

WHEREAS the third and fourth paragraphs of the said section stipulate that a draft of a regulation must be published in the *Bulletin de l'Autorité des marches financiers* with the notice required under section 10 of the Regulations Act (chapter R-18.1) and that the draft of the regulation may not be submitted for approval before 30 days have elapsed since the publication of the draft;

WHEREAS the fifth paragraph of the said section stipulates that a regulation under this section comes into force on the date of its publication in the *Gazette officielle du Québec* or on any later date specified in it, that it must also be published in the *Bulletin de l'Autorité des marches financiers* and that, if the regulation published in the *Bulletin de l'Autorité des marches financiers* differs from the one published in the *Gazette officielle du Québec*, the latter prevails;

WHEREAS section 73 de of the said Act stipulates that a regulation made under this Act may specify that a failure to comply with the regulation may give rise to a monetary administrative penalty, that the regulation may define the conditions for applying the penalty and set forth the amounts or the methods for determining them and that the amounts may vary according to the seriousness of the failure to comply, without exceeding the maximum amounts provided for in section 72;

WHEREAS section 485 of the Insurers Act (chapter A-32.1) stipulates that, in addition to other regulations that it may make under this Act, the *Autorité des marches financiers* may, by regulation, determine the standards applicable to authorized insurers in relation to their commercial practices and their management practices and to federations of mutual companies in relation to their management practices;

WHEREAS the first paragraph of section 486 of the said Act stipulates that a regulation made under this Act by the *Autorité des marches financiers* is approved by the Minister of Finance with or without amendment;

WHEREAS the third and fourth paragraphs of the said section stipulate that a draft of a regulation must be published in the *Bulletin de l'Autorité des marches financiers* with the notice required under section 10 of the Regulations Act (chapter R-18.1) and that the draft of the regulation may not be submitted for approval and the regulation may not be made before 30 days have elapsed since the publication of the draft;

WHEREAS the fifth paragraph of the said section stipulates that a regulation under this section comes into force on the date of its publication in the *Gazette officielle du Québec* or on any later date specified in it, that it must also be published in the *Bulletin de l'Autorité des marches financiers* and that, if the regulation published in the *Bulletin de l'Autorité des marches financiers* differs from the one published in the *Gazette officielle du Québec*, the latter prevails;

WHEREAS section 496 of the said Act stipulates that the *Autorité des marches financiers* may, in a regulation made under this Act, specify that a failure to comply with the regulation may give rise to a monetary administrative penalty, that the regulation may define the conditions for applying the penalty and set forth the amounts or the methods for determining them and that the amounts may vary according to the seriousness of the failure to comply, without exceeding the maximum amounts provided for in section 494;

WHEREAS section 601.1 of the Act respecting financial services cooperatives (chapter C-67.3) stipulates that the *Autorité des marches financiers* may, by regulation, determine the standards applicable to financial services cooperatives in relation to their business and management practices;

WHEREAS the first paragraph of section 601.2 of the said Act stipulates that a regulation made under section 601.1 by the *Autorité des marches financiers* is approved by the Minister of Finance with or without amendment;

WHEREAS the third and fourth paragraphs of the said section stipulate that a draft of a regulation must be published in the *Bulletin de l'Autorité des marches financiers* with the notice required under section 10 of the Regulations Act (chapter R-18.1) and that the draft of the regulation may not be submitted for approval and the regulation may not be made before 30 days have elapsed since the publication of the draft;

WHEREAS the fifth paragraph of the said section stipulates that a regulation under this section comes into force on the date of its publication in the *Gazette officielle du Québec* or on any later date specified in it, that it must also be published in the *Bulletin de l'Autorité des marches financiers* and that, if the regulation published in the *Bulletin de l'Autorité des marches financiers* differs from the one published in the *Gazette officielle du Québec*, the latter prevails;

WHEREAS section 601.9 of the said Act stipulates that the *Autorité des marches financiers* may, in a regulation made under this Act, specify that a failure to comply with the regulation may give rise to a monetary administrative penalty, that the regulation may define the conditions for applying the penalty and set forth the amounts or the methods for determining them and that the amounts may vary according to the seriousness of the failure to comply, without exceeding the maximum amounts provided for in section 601.7;

WHEREAS the paragraph *u* of section 43 of the Deposit Institutions and Deposit Protection Act (chapter I-13.2.2) stipulates that, in addition to the regulatory powers assigned to it by this Act, the *Autorité des marches financiers* may make regulations for determining the standards applicable to authorized deposit institutions in relation to their commercial practices and their management practices;

WHEREAS the first paragraph of section 45 of the said Act stipulates that a regulation of the *Autorité des marches financiers* under this Act must be submitted for approval to the Minister of Finance, who may approve it with or without amendment;

WHEREAS the third paragraph of the said section stipulates that a draft of a regulation referred to in the first paragraph may not be submitted for approval and the regulation may not be made before the expiry of 30 days after the publication of the draft regulation and that the regulation comes into force on the date of its publication in the *Gazette officielle du Québec* or on any later date determined in the regulation;

WHEREAS section 45.9 of the said Act stipulates that the *Autorité des marches financiers* may, in a regulation made under this Act, specify that a failure to comply with the regulation may give rise to a monetary administrative penalty, that the regulation may define the conditions for applying the penalty and set forth the amounts or the methods for determining them and that the amounts may vary according to the seriousness of the failure to comply, without exceeding the maximum amounts provided for in section 45.7;

WHEREAS section 277 of the Trust Companies and Savings Companies Act (chapter S-29.02) stipulates that in addition to other regulations that it may make under this Act, the *Autorité des marches financiers* may, by regulation, determine the standards applicable to authorized trust companies in relation to their commercial and management practices;

WHEREAS the first paragraph of section 278 of the said Act stipulates that a regulation made under this Act by the *Autorité des marches financiers* is approved by the Minister of Finance with or without amendment;

WHEREAS the third and fourth paragraphs of the said section stipulate that a draft of a regulation must be published in the *Bulletin de l'Autorité des marches financiers* with the notice required under section 10 of the Regulations Act (chapter R-18.1) and that the draft of the regulation may not be submitted for approval and the regulation may not be made before 30 days have elapsed since the publication of the draft;

WHEREAS the fifth paragraph of the said section stipulates that a regulation under this section comes into force on the date of its publication in the *Gazette officielle du Québec* or on any later date specified in it, that it must also be published in the *Bulletin de l'Autorité des marches financiers* and that, if the regulation published

in the *Bulletin de l'Autorité des marches financiers* differs from the one published in the Gazette officielle du Québec, the latter prevails;

WHEREAS section 286 of the said Act stipulates that the *Autorité des marches financiers* may, in a regulation made under this Act, specify that a failure to comply with the regulation may give rise to a monetary administrative penalty, that the regulation may define the conditions for applying the penalty and set forth the amounts or the methods for determining them and that the amounts may vary according to the seriousness of the failure to comply, without exceeding the maximum amounts provided for in section 284;

WHEREAS the draft Regulation respecting the management and reporting of information security incidents by certain financial institutions and by credit assessment agents was published in the *Bulletin de l'Autorité des marchés financiers*, volume 20, no. 48 of December 7, 2023;

WHEREAS the *Autorité des marches financiers* made, on September 16, 2024, by the decision no. 2024-PDG-0043, Regulation respecting the management and reporting of information security incidents by certain financial institutions and by credit assessment agents;

WHEREAS there is cause to approve this regulation without amendment;

CONSEQUENTLY, the Minister of Finance approves without amendment Regulation respecting the management and reporting of information security incidents by certain financial institutions and by credit assessment agents appended hereto.

October 7, 2024

ERIC GIRARD
Minister of Finance

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 that may occur within the institution, a credit union that is a member of a federation, the credit assessment agent, or a third party to which such institution, credit unition that is a member of a federation, or credit assessment agent has entrusted the performance of any part of an activity, if the incident affects the activity entrusted to such third party.

The information security incident management policy shall also contain a procedure for the reporting of information security incidents to the officers or, where applicable, 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 referred to in the first paragraph.

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, one of its managers.

DIVISION II
REPORTING TO THE AUTORITÉ DES MARCHÉS FINANCIERS

5. Where an information security incident with potentially adverse impacts is reported to the officers or, where applicable, the managers of a financial institution or a credit assessment agent, the financial institution or the credit assessment agent must, not later than 24 hours from the time the incident is so reported, notify the Authority of the incident.

The financial institution or the credit assessment agent must, within that same period, also notify the Authority of any information security incident that has been reported or been the subject of a notice 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. Where 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 notify the Authority of the incident at the same time.

7. A financial institution or a credit assessment agent shall notify the Authority of an information security incident 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 not later than three days after notice is given to the Authority pursuant to section 5 and not later than every three days thereafter, until a notice is sent to the Authority confirming that the incident is under control and that operations have returned to normal.

9. A financial institution or a credit assessment agent shall send a report to the Authority within 30 days following the date the notice is sent to the Authority confirming that the incident is under control and that operations have returned to normal. The report shall, in particular:

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

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

(3) describe the actions taken to reduce the likelihood of incidents of a similar nature occurring in the future.

DIVISION III
INFORMATION SECURITY INCIDENT REGISTER

10. A financial institution or a credit assessment agent must maintain a current information security incident register that shall include, 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 9;

(5) any injury caused by the incident;

(6) any third parties involved in the incident;

(7) actions taken;

(8) whether the residual risk is accepted or not accepted and the rationale for accepting or not accepting it;

(9) planned actions; and

(10) the incident close date.

11. 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 five years from the date of the report referred to in section 9.

CHAPTER III
MONETARY ADMINISTRATIVE PENALTIES

12. 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, fails to assign, in writing, responsibility for monitoring the management and reporting of information security incidents to one of its officers or, where applicable, one of its managers;

(2) in contravention of section 5, fails to notify the Authority of an incident not later than 24 hours after the time the incident is reported to its officers or, where applicable, its managers;

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

(4) in contravention of section 8, fails to notify the Authority of developments in the situation not later than three days following the notice referred to in section 7 and not later than every three days thereafter, until a notice is sent to the Authority confirming that the incident is under control and operations have returned to normal.

13. 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 10, fails to maintain a current information security incident register; or

(3) in contravention of section 11, fails to keep the information in the information security incident register for a minimum period of five years from the date of the report contemplated in section 9.

CHAPTER IV
FINAL PROVISION

14. This Regulation comes into force on (*indicate the date that is six months after the date of its publication in the Gazette officielle du Québec*).

107061