Draft Regulation

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)

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

Notice is hereby given by the Autorité des marchés financiers (the "Authority") that, in accordance with section 67 of the Credit Assessment Agents Act, CQLR, c. A-8.2 (the "CAAA"), section 486 of the Insurers Act, CQLR, c. A-32.1, section 601.2 of the Act respecting financial services cooperatives, CQLR, c. C-67.3 (the "AFSC"), section 45 of the Deposit Institutions and Deposit Protection Act, CQLR, c. I-13.2.2 (the "DIDPA"), and section 278 of the Trust Companies and Savings Companies Act, CQLR, c. S-29.02 (the "TCSCA"), the following regulation (the "Draft Regulation"), the text of which is published hereunder, may be made by the Authority and subsequently submitted to the Québec Minister of Finance for approval, with or without amendment, after 75 days have elapsed since its publication in the Bulletin of the Authority:

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

The Draft Regulation is also available under "Public consultations" on the Authority's website at **www.lautorite.qc.ca**.

Background

The Draft Regulation fits within the Authority's mission to ensure that financial institutions have sound and prudent management practices that support their resilience. The Draft Regulation also fits within the Authority's mission in relation to credit assessment agents ("CAAs") and its mandate to supervise and control their management practices. Developing and maintaining sound management practices helps financial institutions and CAAs prevent and manage incidents that could cause them injury, harm their reputation or, in the case of financial institutions, jeopardize their solvency.

Purpose of the Draft Regulation

The Draft Regulation applies to the following financial institutions and CAAs:

Financial institutions

- Insurers authorized under the Insurers Act and federations of mutual companies governed by the Insurers Act;
- Federations and credit unions not members of a federation that are subject to the AFSC;
- Deposit institutions authorized under the DIDPA;
- Trust companies authorized under the TCSCA.

Credit assessment agents

- CAAs designated by the Authority under the CAAA.

1. Application

The Draft Regulation proposes a framework for the management and reporting of information security incidents ("incident(s)") that may occur within a financial institution, a CAA or a third party entrusted with the performance of any part of an activity.

It is proposed that, where there is a federation and its member credit unions, the proposed obligations in the Draft Regulation would apply to the federation. The federation would be responsible for, among other things, developing and implementing a policy for the reporting of incidents to its managers and the Authority, including incidents that may occur within a member credit union.

It is also proposed that the Draft Regulation would apply to a federation of mutual companies and to each company that is a member of the federation.

2. Information security incident management policy

The Draft Regulation proposes requiring, among other things, that CAAs and financial institutions develop and implement an incident management policy. The policy would have to include procedures and mechanisms for detecting, assessing and responding to incidents. It would also have to include a procedure for the reporting of incidents to the officers[1] of the financial institution or the CAA and to any stakeholders.

3. Reporting to the Autorité des marchés financiers

Any incident with potentially adverse impacts that a CAA or a financial institution reports to its officers or, as the case may be, to its managers would have to be reported to the Authority no later than 24 hours after it occurs.

Also, the Authority must be notified, within that same period, of any incident that is reported to another regulatory authority, 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. Accordingly, any incident reported to the Office of the Superintendent of Financial Institutions ("OSFI"), the police or an insurer covering cyber risk would have to be reported to the Authority.

Any confidentiality incident for which notification is sent to the Commission d'accès à l'information must be reported to the Authority at the same time.

4. Information security incident register

The financial institution or the CAA would be required to maintain a current incident register that includes, for each incident, a description of the incident, any injury caused by it, the third parties involved in it, acceptance of the residual risk, actions taken, planned actions and the incident close date. The information recorded in the incident register would have to be kept in a secure and confidential manner so as to maintain the integrity of the information for a minimum period of seven years.

[1] In the case of a federation, the incident would have to be reported to the managers within the meaning of the AFSC.

5. Monetary administrative penalties

Lastly, the Draft Regulation sets out monetary administrative penalties that the Authority may impose on a financial institution or a CAA that contravenes the provisions of the Draft Regulation. Penalties will be imposed according to the statutory provisions applicable to the contravening financial institution or CAA. A notice of non-compliance would have to be sent before a penalty is imposed.

The obligations set out in the Draft Regulation adds to the Authority's guideline expectations for financial institutions and CAAs relating to their obligation to adhere to management practices but does not replace them.

Comments

Comments regarding this Draft Regulation may be made in writing before **February 20, 2024** to:

Me Philippe Lebel
Corporate Secretary and Executive Director, Legal Affairs
Autorité des marchés financiers
Place de la cité, tour Cominar
2640, boulevard Laurier, 3ème étage
Québec (Québec) G1V 5C1
Fax: 418-525-9512
E-mail: consultation-en-cours@lautorite.qc.ca

Unless otherwise noted, comments will be posted on the Authority's website at www.lautorite.qc.ca. Please do not include personal information directly in comments to be published and state on whose behalf you are making the submission.

Additional Information

Additional information may be obtained from:

Isabelle Déry
Financial Institution Standardization Analyst
Prudential Policy and Simulations
Autorité des marchés financiers
Telephone: 418-525-0337, ext. 4176
Toll-free: 1-877-525-0337
Isabelle.dery@lautorite.qc.ca

Luc Verreault
Financial Institution Standardization Analyst
Prudential Policy and Simulations
Autorité des marchés financiers
Telephone: 514-395-0337, ext. 4644
Toll-free: 1-877-525-0337
Luc.verreault@lautorite.qc.ca

December 7, 2023