Submitted by email to: consultation-en-cours@lautorite.qc.ca

Montreal, February 13, 2025

Philippe Lebel
Corporate Secretary and Executive Director, Legal Affairs
Autorité des marchés financiers
Place de la Cité
2640, boulevard Laurier, bureau 400
Québec (Québec) G1V 5C1

Re: Consultation on the AMF's new form for reporting information security incidents

Dear Mr. Lebel,

The Canadian Life and Health Insurance Association (CLHIA) is pleased to provide feedback as part of the consultation process on the information security incident reporting form as it pertains to the *Regulation respecting the management and reporting of information security incidents by certain financial institutions and by credit assessment agents* published in the Autorité des marchés financiers (AMF) Bulletin on January 16, 2025.

Below you'll find our general comments on the form and specific recommendations for certain sections.

GENERAL COMMENTS

In the event that a financial institution subject to the Regulation experiences an information security incident, it will be subject to various reporting requirements on the part of regulators.

The institution will need to use the form discussed herein to notify the AMF of such incidents, provide updates, and submit a final report once the situation is under control.

Federally chartered financial institutions will also need to report the incident to the Office of the Superintendent of Financial Institutions (OSFI) using a separate information security incident reporting form.

If the incident involves a breach of confidentiality, organizations will also be required, under certain conditions, to notify Quebec's Commission d'accès à l'information.[1]

[1] Section 3.5 of the *Act respecting the protection of personal information in the private sector*.

We recognize that Canada's various governing bodies and legal authorities each have their own mandates and requirements. However, in a context where we aim to limit the regulatory and administrative burden on organizations to foster greater efficiency and agility, we urge the AMF to work with its federal and provincial counterparts to create a single Canada-wide form for reporting information security incidents.

In its Recommendations to Achieve Greater Convergence in Cyber Incident Reporting: Final Report, published in April 2023, the Financial Stability Board stated that "*financial authorities should individually or collectively identify common data requirements and, where appropriate, develop or adopt standardized formats for the exchange of incident reporting information*."

We believe this would help organizations establish more effective security incident reporting policies and ultimately allow them to better manage security incidents.

SPECIFIC COMMENTS

Incident type

The taxonomy proposed in the AMF form raises a number of issues that we'd like to address below.

a. Categories that are not mutually exclusive

The proposed taxonomy of incident types includes categories that are not mutually exclusive. For example, if an organization receives a phishing email with a link that, once clicked on, runs a malicious command that provides access to its local system (unauthorized access) and potentially triggers a ransomware command, which incident type should the organization select?

Will organizations be able to select multiple categories or will they be limited to one? If they can only select one, should they select the one that describes the initial type of incident, the type of command triggered, or the final action performed?

b. Definitions of incident types

In our view, the incident types in the form are more akin to incident causes. For example, "human error," the "vulnerability" of a computer system, and "social engineering" are possible causes of incidents rather than types of incidents.

In other jurisdictions, those elements are considered possible causes of an information security incident. To avoid confusion over terminology, the list of incident types should be reviewed.

We recommend that "human error," "vulnerability" of a computer system, and "social engineering" be removed from the list of possible incident types and included as examples in the section on incident causes.

c. Clarification for some incident types

Some of the proposed incident types also need clarification. This is particularly the case for "Fraud," which from an operational standpoint isn't a type of information security incident, but rather the result of such an incident. **We recommend that this option be removed from the list of incident types**.

In addition, we'd like "System outage" and "System error" to be clarified in order to better understand the AMF's expectations regarding those incident types.

Dates and times when the incident was detected and occurred

In general, we question the need to specify the time at which a security incident occurred or was detected. Tracking down that very specific information complicates the reporting process. **We recommend that only the occurrence and detection dates be required in order to simplify the reporting process**.

In some cases, an incident may occur several times before it is detected. That makes it difficult to identify the exact time when the incident first occurred.

We propose that institutions be allowed to indicate a period of time in the "Date and time incident occurred" section, or at least clarify that the occurrence reported in the form is not necessarily the first.

Incident status

The AMF form provides three options for indicating the current status of an incident: "Open," "Under control," and "Closed." When an organization notifies the AMF that the incident is under control, it is automatically given 30 days to submit the post-mortem report so the incident can be closed.

However, in certain situations, a security incident could be described as being under control because operations have returned to normal, but the incident analysis is still ongoing and the organization needs more than 30 days to provide the documentation required to close the incident.

For example, an incident involving the confidentiality of information—such as unauthorized access to an email inbox—could take more than 30 days to investigate but cause no operational disruption.

We'd like to draw the AMF's attention to the fact that some incidents may require more than 30 days to complete the necessary analyses for the post-mortem report.

Dates and times when the incident was brought under control and closed

In connection with our previous point, it can be difficult for organizations to provide information about when an incident was closed, since in some situations an incident could be under control but still under investigation within the organization. A period of 30 days may therefore not be sufficient for organizations to meet the regulatory requirements for providing a post-mortem report.

Having to specify the time at which an incident was brought under control and the time at which it was closed complicates the reporting process without adding value.

We therefore recommend that the requirement to specify the time at which an incident was brought under control and the time at which it was closed be removed.

Parties

Identifying the parties involved in the incident raises a number of issues and we'd like to propose the following changes:

a. Names of the parties involved in the incident

The form requires that "*all known internal and external parties involved in the incident"* be identified and gives *"employee or consultant within the organization*" as an example.

We recommend that organizations be required to identify the roles of the people involved within particular teams rather than their first and last name. Specifying names adds no value, and this would simplify the process.

The AMF's explanation on the form could be changed as follows:

> "Please identify all known internal and external parties involved in the incident (e.g., ~~employee or consultant~~ team or department within the organization, recognized malicious organization), […]"

b. Location of the parties involved in the incident

Could the AMF specify what information it expects regarding the location of the parties involved in the incident?

Date and time when the incident was reported to the stakeholders, as required by the Regulation

a. Suggested changes

To clarify the AMF's expectations and help organizations comply with this section, we'd like to suggest some changes:

- Add the following to clarify and define the reporting referred to in the form:

  "Please specify the date and time you reported the incident to any of the following parties as per the reporting criteria in your incident management policy:"

- In the stakeholder list, update the wording for consistency and to better define the AMF's expectations:

"Officers or, where applicable, managers (senior management)." This would make that wording consistent with the wording in the previous section of the form.

"*Third parties to which your organization has entrusted the performance of any part of an activity, if the incident affects the activity entrusted to such third party."* This would better define the third parties concerned and make that wording consistent with the wording in the Regulation.

- Remove the requirement in the Regulation to specify the time at which the incident was reported to stakeholders. This complicates the reporting process for organizations and doesn't appear to add value.

b. Request for clarification

In the case of a confidentiality incident, organizations report to the Commission d'accès à l'information (CAI) once they have gathered sufficient information and established the impact on customers. This means that some information security incidents involving confidentiality issues could be disclosed to the AMF before they're disclosed to the CAI.

How does the AMF expect organizations to provide information about when they reported an incident to the CAI if they do so after notifying the AMF?

Nature and volume of clients affected

Can the AMF clarify what is meant by *"transactions affected by the incident"* and *"geographical distribution"* in the explanatory text?

Reactions of the public or other stakeholders

As worded in the form, this section is very broad in scope and would be difficult to comply with. We suggest the following changes to help better define the request:

- Limit the expectations in this part of the form to reactions from the public and remove "*or other stakeholders*" from the section heading.

- Furthermore, not all reported incidents will elicit a reaction from the public. We therefore suggest the following change to the descriptive text in the form:

"Nature and origin of the reactions ~~of the various external stakeholders~~ from the public known to date, if any."

External communications issued to date

This section seems to duplicate the section earlier in the form where organizations are asked to indicate the date and time incidents were reported to stakeholders, as required by the Regulation.

The scope of this section also appears to be very broad. We recommend that it be narrowed to focus on general external communications issued by the organization and therefore exclude communications specifically addressed to suppliers and customers affected by the incident.

Residual risk

We recommend that this section heading be changed to "*Recurrence potential*" to clarify what is meant by "*residual risk*" and make the objective of this section of the form clearer.

CONCLUSION

Thank you for the opportunity to comment on your form for reporting information security incidents. We remain available for further discussion. Please direct all enquiries to Typhaine Letertre, Director, Public Policy, at tletertre@clhia.ca.