BANK OF CANADA
BANQUE DU CANADA

Guideline consultation

The *Retail Payment Activities Act* (RPAA) and the *Retail Payment Activities Regulations* (RPAR) require payment service providers to meet specific risk management and notification requirements. The RPAA also provides the Bank of Canada with the authority to issue guidelines that set out the manner in which the Bank expects the Act to be applied.

The Bank's guidelines outline the standards and practices that payment service providers are expected to incorporate into their business operations to support their compliance with the RPAA and RPAR. The Bank may conduct consultations on its guidelines to gather input and feedback on these supervisory expectations.

The Bank is seeking your feedback to inform the final version of this guideline. We are specifically interested in obtaining feedback on aspects of the draft guideline that could be:

- clarified
- challenging to implement

We also welcome any additional comments related to the standards and practices outlined in the draft guideline. Please note, the Bank is *not* seeking feedback on regulatory concepts in the RPAA or RPAR, as both the legislation and the regulations have been finalized by the Government of Canada and the Department of Finance Canada.

The Bank expects to publish a final version of this guideline in the second half of 2024.

Submitting your comments

Please submit your comments to RPSconsultationsSPD@bank-banque-canada.ca by May 21, 2024. In order for the Bank to have sufficient time to review and analyze the feedback and finalize the guideline, any comments submitted after this date may not be considered. An anonymized summary of comments will accompany the final published guidelines. During the consultation period, the Bank may engage directly with respondents to obtain more information.

To provide comments on the other draft guidelines currently open for consultation, please visit the RPS Guideline Consultation page: https://www.bankofcanada.ca/rps-consultation/.

The Bank is subject to the Access to Information Act (AIA). The AIA provides that information that is shown to be confidential or could be shown to prejudice the competitive position of a third party must be protected. Should the Bank receive a request for information supplied by your organization, the Bank will maintain the confidentiality of the information to the extent possible, by law.

BANK OF CANADA
BANQUE DU CANADA

Incident notification

Type of publication: Draft supervisory guideline for consultation

Introduction

Under the *Retail Payment Activities Act* (RPAA), if a payment service provider (PSP) becomes aware of an incident that has a material impact on an end user, another PSP or a clearing house of a clearing and settlement system, the PSP must, without delay, notify the affected individuals or entities and the Bank of Canada. This supervisory guideline explains the requirements on incident reporting and provides clarity, when appropriate, on how the Bank expects PSPs to comply with those regulatory requirements.

1. Context

1.1 As set out in the *Retail Payment Activities Regulations* (RPAR) and the *Operational risk and incident response* guideline, PSPs must take immediate action to respond to incidents. All incidents, regardless of their impact, must be investigated, responded to and documented.

1.2 Under subparagraph 5(1)(i)(iii) of the RPAR, upon becoming aware of an incident, the PSP must immediately investigate it. As part of the investigation, the PSP must determine the incident's possible or verified impact on end users, other PSPs and clearing houses.

1.3 Under section 18 of the RPAA, if it is determined that the incident has a material impact, the PSP must, without delay, notify the affected end users, other PSPs, clearing houses and the Bank.

- An end user, as defined in section 2 of the RPAA, is an individual or entity that uses a payment service as a payer or payee.
- A PSP refers to any PSP, regardless of whether or not the RPAA applies to that individual or entity. Refer to the *Criteria for registering payment service providers* supervisory policy.
- A clearing house means a clearing house of a clearing and settlement system, as defined in section 2 of the *Payment Clearing and Settlement Act*, that is designated under subsection 4(1) of that Act. See the Bank's website for information on designated financial market infrastructures (FMIs).

1.4 Incidents that do not have a material impact on the individuals or entities noted in section 1.2 of this guideline are not subject to the reporting requirements under section 18 of the RPAA. However, the Bank may request information separately about such incidents to assess a PSP's compliance with section 18 of the RPAA and with its operational risk management obligations under section 17 of the RPAA.

2. PSP incidents

2.1 An incident, as defined in section 2 of the RPAA, is "an event or series of related events that is unplanned by a payment service provider and that results in, or could reasonably be expected to result in, the reduction, deterioration, or breakdown of any retail payment activity that is performed by the payment service provider."

2.1.1 The Bank's view is that a "reduction, deterioration, or breakdown," as used in this definition, occurs, but is not limited to, when there is a negative impact on the confidentiality, integrity or availability of:

- a PSP's retail payment activities; or
- the systems, data and information involved in the PSP's performance of those activities.

2.1.2 As set out in the *Operational risk and incident response* guideline:

- **Integrity** refers to accuracy and completeness: no improper modification or destruction of a system, data or information.
- **Confidentiality** refers to ensuring that data or information is neither made available nor disclosed to unauthorized individuals, entities, processes or systems; preserving authorized restrictions on data and information access and disclosure.
- **Availability** refers to services being accessible and usable on demand by an authorized entity; ensuring timely and reliable access to and use of a payment service, system, data or information.

2.1.3 Incidents may include events that occur at or are detected by a PSP's agents and mandataries or a PSP's third-party service providers. PSPs are required to report incidents that occur at or are detected by their agents and mandataries and third-party service providers.

3. Incidents with material impact

3.1 Only incidents that have a material impact on an end user, a PSP or a clearing house are subject to the notification requirement in section 18 of the RPAA. An incident is subject to these requirements if one or more of these parties is affected. Some examples of incidents that could have a material impact on an end user, PSP or clearing house of a designated clearing and settlement system, and the circumstances that could give rise to them are listed below.

3.1.1 Any amount of an end user's funds held by a PSP has become lost or unavailable before the end user withdraws those funds or transfers them to another individual or entity. Examples of incidents that could have this impact could include:

- end-user funds are stolen; or
- the provider of the account used to hold end-user funds has either ceased operations or is in some form of financial distress, and end-user funds held in that account are not accessible by end users in part or in full.

3.1.2 The PSP experiences an outage of or slowdown in its retail payment activities for eight or more hours. An outage or slowdown occurs when any task, process or system related to the provision of a PSP's retail payment activities is down and thus prevents or inhibits the provision of those retail payment activities to one or more end users (such as the inability to access payment account) or affects another PSP or a clearing house. Examples of incidents that would have this impact could include:

- technology failure;
- loss of data centre;
- loss of infrastructure hosting service;
- loss of third party; or
- cyber attack.

3.1.3 The PSP is subject to an insolvency proceeding event referred to in subsection 14(3) of the RPAR.

3.1.4 The confidential information of an end user, a PSP or a clearing house is accessed or disclosed without authorization, resulting in or creating a real risk of significant harm to the end user, PSP or clearing house. Significant harm includes:

- bodily harm;
- humiliation;
- damage to reputation or relationships;
- loss of employment, business or professional opportunities;
- financial loss;
- identity theft;
- negative effects on the credit record; or
- damage to or loss of property.

A PSP should assess the risk of significant harm that could arise from a breach of any data or information that the PSP has determined should remain confidential. To determine whether a breach (that is, an unauthorized access or disclosure of confidential information) results in or creates a real risk of significant harm to an end user, a PSP or a clearing house, the PSP should consider:

- the sensitivity of the information involved in the breach; and
- the probability that the information has been, is being or will be misused.

3.1.5 The integrity of the PSP's retail payment activities is compromised. Examples of incidents that would have this impact could include:

- compromise to the PSP's ledger (as described in *Safeguarding end-user funds* guidelines);
- compromise of transaction records;
- transaction processing errors (for example, payer sends $5 but payee receives $3);
- incorrect routing of end-user funds (that is, funds are not deposited into end user's account as expected);
- misdirection of instructions related to an electronic funds transfer;
- improper calculation at clearing or settlement;
- unauthorized changes to or deletion of other data or information.

3.1.6 An incident could have a material impact in multiple ways: that is, more than one threshold set out in the examples of section 3 is met. In other words, the materiality thresholds could overlap (for example, an incident compromises the integrity of a PSP's ledger, which results in end-user funds being lost).

4. Reporting incidents

4.1 Incidents that have a material impact must be reported to the affected end user, PSP or clearing house and the Bank without delay, but no later than 24 hours after the PSP becomes aware of the incident.

4.1.1 If an incident does not meet the materiality thresholds referred to in the examples in section 3 of this guideline when first detected but progresses in severity over time, it should be reported without delay, but no later than 24 hours from the point at which it is determined to be a material incident.

Reporting incidents to the Bank of Canada

4.2 Any incident that has a material impact on an end user, PSP or clearing house must be reported to the Bank using the incident reporting template.

4.3 Under section 11 of the RPAR, PSP's incident report to the Bank must include the following information:

4.3.1 The PSP's contact information, including:

- the name of the PSP; and
- a primary contact from the PSP that would be able to clarify information about the incident, if the Bank requires it, and their contact information (phone number, email address).

4.3.2 A description of the incident and its material impact on end users, PSPs or clearing houses. The description should include:

- date and time the incident started;
- date and time the incident was detected;
- if different from the date and time it was detected, the date and time it was determined that the incident has progressed from a non-material to a material incident, as described in the examples in section 3 of this guideline;
- date and time when the incident was resolved (ended);
- how the incident was detected: for example, a report from an end user or detection by the PSP or a third-party service provider;
- brief description of the incident, including what the specific issue is and which retail payment activities have been affected;
- details on the nature of actual or estimated impact of the incident on end users, other PSPs or clearing houses: for example, the number of persons or entities affected;

4.3.3 Measures taken to date to respond to the incident: for example, internal escalation.

4.4 The Bank may require that a PSP issue a follow-up notice, as authorized under subsection 19(1) of the RPAA, if the Bank determines that more information about an incident is required or should be reported to other persons or entities.[1]

4.4.1 In these cases, the follow-up notice order will set out who the notice must be given to (for example, the Bank, all end users, particular end users), when the follow-up notice must be given and how, and the information that must be included in the notice at the time the order is issued by the Bank.

4.4.2 The contents of the follow-up notice would depend on the incident at hand because it will need to reflect the individual circumstances of the incident.

---

1 The Bank may also request additional information using an information request, under subsection 65(1) of the RPAA. In accordance with subsection 43(2) of the RPAR, the PSP has 24 hours to respond if the information requested by the Bank relates to an ongoing incident that could have a significant adverse impact on an end user; on a PSP, whether or not the RPAA applies to it; or on a clearing house of a clearing and settlement system that is overseen by the Bank under the *Payment Clearing and Settlement Act*.

4.4.3 A PSP may be required to issue follow-up notices more than once to materially affected individuals or entities, if deemed necessary, until all relevant details about the incident have been provided.

Reporting incidents to affected end users, payment service providers and clearing houses

4.5 Under section 12 of the RPAR, a PSP is required to notify all materially affected end users, PSPs and clearing houses.

- When a materially affected end user, PSP or clearing house has provided contact information to the PSP, the PSP must notify that individual or entity using that individual's or entity's most recent contact information.
- When the PSP does not have contact information for every materially affected end user, PSP or clearing house, the PSP is required to publish a notice on its website.
- To facilitate incident notifications without delay, it is recommended that a PSP maintain up-to-date contact information for its end users and for the PSPs and clearing houses they are connected with.

4.5.1 For clarity, when an incident at a PSP materially affects another PSP that performs retail payment activities, the affected PSP is required to notify its end users if those end users are materially affected by the incident. For example, if PSP A were to experience an incident that materially affects both its end users and PSP B, which then materially affects PSP B's end users, PSP A would need to notify all its affected end users and PSP B of the incident. PSP B would also be responsible for notifying its affected end users if the incident meets the criteria for a material incident at PSP B.

4.6 Notices from the PSP about an incident should be provided to each materially affected end user, PSP or clearing house without delay, no later than 24 hours from detection of the incident, using available contact information.

4.6.1 The Bank expects such notices to be provided directly to the materially affected end user, PSP or clearing house.

4.6.2 For example, electronic notifications of an incident by email, text message, or the PSP's app or website (in cases where the PSP has no contact information of the materially affected end user, PSP or clearing house) would be suitable, whereas posting on social media would not be considered an appropriate means of incident notification.

4.6.3 However, if a PSP wishes to provide notice of an incident on social media in addition to sending an email to an end user, for example, the Bank's expectations do not prevent a PSP from doing so.

4.7 Under Section 12 of the RPAR, a PSP's incident notice to materially affected end users, PSPs and clearing houses must include the following information:

4.7.1 the PSP's name;

4.7.2 a description of the incident and its impact on end users, PSPs or clearing houses that includes:

- date and time the incident started;
- date the incident was detected;
- date the incident was resolved (ended);
- details on the nature of the actual or estimated impact of the incident on the end user, PSP or clearing house being notified of the incident;

4.7.3 corrective measures that can be taken by the materially affected individuals or entities to mitigate any adverse effects of the incident, if applicable (for example, change password).

4.8 Note that PSPs, as participants in clearing and settlement systems, may be subject to incident reporting requirements from both the Bank under the RPAA as well as under the rules or contractual arrangements related to participation in the clearing and settlement system.

If this is the case, and a PSP is reporting incidents to a clearing house under criteria established as part of the clearing house's participation obligations, and those criteria are different from what has been established by the Bank under the RPAA, the clearing house may choose to request that a PSP provide incident reports under its own criteria only or may choose to receive all reports under the RPAA as well as the reports under its own criteria.

4.8.1 In either case, all material incidents as defined in this guidance must be reported to the Bank.

4.8.2 Meeting the Bank's incident reporting obligations would not exempt a PSP from meeting obligations established as part of its membership of these clearing houses or any other reporting obligations.

4.9 If an incident would be captured by both the Bank's incident reporting requirements and relevant federal or provincial privacy laws (for example, confidentiality breaches of personal information that create a real risk of significant harm to the person or entity), the PSP is still required under the RPAA to notify the Bank and materially affected individuals or entities.