Public Consultation Report: Interim Retail Payments Advisory Committee (RPAC)

August 26 & 27, 2020

Summary

The Interim Retail Payments Advisory Committee (RPAC) held its third meeting on August 26 & 27, 2020. Participants continued their discussion on business practices for operational risk management.

Who we consulted

Participants:	**Method of engagement:**	**Purpose of engagement:**
• Bank of Canada • Department of Finance • Moneris • Nanopay • PayPal • Paytm (regrets) • Square • STACK (regrets) • Telpay • TransferWise • Visa • Western Union	Virtual (Webex)	To facilitate the Bank of Canada's understanding of the retail payments ecosystem and current operational risk practices of payment service providers (PSPs).

What we asked

- Participants were asked:
  - What types of systems are used to support retail payment activities and thus could be scoped into operational risk expectations;
  - What factors drive their objectives regarding operational availability;
  - What their key operational risks are and the sources of those risks;
  - How operationally critical assets are identified;
  - How they prioritize investment in protective controls;
  - What challenges they face to protect data in transit; and,
  - To discuss their approach to BCP planning and resourcing.
- Detailed questions of what was asked can be found in the discussion guide for this event.

What we heard

- Data and systems that are used in, or are critical to, the provision of retail payment service should be scoped in. Additional clarity on the criteria for data and systems that would be in scope would be welcome.

- Most participants have availability targets.
    - Targets are primarily driven by customer expectations.
    - Targets are agreed to contractually with external service providers.
    - PSPs are not "systemically important" entities, and consequently non-availability is less impactful.
    - Members are not currently subject to regulatory requirements that prescribe minimum availability targets.
- A principles-based approach to regulatory requirements concerning risk identification is preferred. A principles-based approach better accommodates the evolving nature of operational risk and the differences among PSPs.
    - Participants identified third-party risk and fraud as major risks to their business, in addition to the risks set out in the discussion guide.
- Most participants perform asset criticality assessments.
    - Additional clarity on asset criticality perspectives may be helpful, as different assets can be deemed critical from different lenses (e.g., certain assets are considered critical from a business continuity perspective, whereas other assets may be considered critical from a cyber security perspective).
- PSPs primarily take a holistic, risk-based approach to investing in operational risk mitigation, which could span across protective, detective, and responsive controls. Risk is examined holistically to determine where the largest vulnerabilities exist (e.g., biggest impact on customers) and controls are then employed to mitigate that risk.
    - There is more investment in controls for critical assets or critical services that, in the absence of the asset or service, would have a significant negative impact on customers.
    - Certifications (e.g. PCI Security Standards) can drive investment in protective controls, and are contractually required by some business partners or customers.
- Protection of data in transit, at use, and at rest:
    - Participants noted that clear protocols exist to protect data in transit (e.g., encrypted).
    - When multiple parties are involved, the liability and responsibility is designated contractually.
    - Participants typically integrate oversight mechanisms into their contractual agreements with third-parties.
    - Participants indicated that federal and provincial data protection laws require them to implement controls to safeguard their data.
- Some participants indicated that their approach to business continuity planning is focused on what would be required to return to operations, rather than developing specific scenarios that would result in a disruption of service. Scenario-based testing exercises are, however, of value to identify gaps in the business continuity plan, and participants conduct such tests on a regular basis.
    - Some participants indicated that their business continuity plan is complemented by a more strategic crisis management plan.
    - Coordinated testing of business continuity arrangements across PSPs is not common practice.

- There can be trade-offs between restoring integrity/confidentiality and maintaining service availability following an operational incident. Although prioritizing one over the other can be situationally dependent, participants expressed the view that maintaining or restoring integrity/confidentiality is the priority.
- Resources for implementing a business continuity plan are typically included within normal operating budgets for both financial, and human resources.
    - Participants indicated that external expertise may be sought out for certain types of incidents (e.g. cyber attacks).
    - Participants did not foresee a problem in accessing such external expertise in the event of an incident, but this could be a challenge for smaller PSPs.

What happens next

- The Bank of Canada will continue to support Finance Canada in developing options managing operational risk under the proposed Retail Payments Oversight Framework.
- Concrete concepts on operational risk will be provided to members to elicit further feedback in an upcoming RPAC session.