Rapport de consultation publique : Comité consultatif intérimaire sur les paiements de détail

Les 26 et 27 août 2020

Résumé

Le Comité consultatif intérimaire sur les paiements de détail a tenu sa troisième réunion les 26 et 27 août 2020. Les participants ont poursuivi leur discussion sur les pratiques de gestion du risque opérationnel au sein de leur filière.

Qui nous avons consulté

Participants :	**Mode de communication :**	**Objectif de la rencontre :**
• Banque du Canada • Ministère des Finances • Moneris • Nanopay • PayPal • Paytm (absent) • Square • STACK (absent) • Telpay • TransferWise • Visa • Western Union	Virtuel (Webex)	Permettre à la Banque du Canada de mieux comprendre l'écosystème des paiements de détail et les pratiques actuelles des fournisseurs de services de paiement dans le domaine de la gestion du risque opérationnel.

Ce que nous avons demandé

- Points sur lesquels les participants ont été interrogés :
  - Quels types de systèmes participent au bon déroulement des opérations de paiement et pourraient de ce fait entrer dans le périmètre des attentes dont relève le risque opérationnel;
  - Quels facteurs déterminent leurs objectifs sur le plan de la disponibilité opérationnelle;
  - Quels sont les principaux risques opérationnels et leurs causes;
  - Comment se fait l'identification des actifs essentiels pour les opérations;
  - Comment sont établies les priorités d'investissement dans les mesures de protection;
  - Quels défis doivent être relevés pour protéger les données qui sont transmises;
  - Approche des fournisseurs pour la préparation et la dotation du plan de continuité des opérations.
- On trouvera dans le guide de discussion le libellé précis des questions qui ont été posées.

Ce qu'on nous a dit

- Les fournisseurs ont parlé des données et des systèmes utilisés ou essentiels pour la prestation des services de paiement de détail qui devraient être visés. Il serait préférable d'obtenir plus de précisions sur les critères présidant au choix des données et des systèmes visés.
- La plupart des participants ont des cibles en matière de disponibilité.
    - Ces cibles sont fixées en tout premier lieu en fonction des attentes des clients.
    - Les cibles font l'objet d'un accord contractuel avec les fournisseurs externes de services.
    - Les fournisseurs de services de paiement n'étant pas des entités d'importance systémique, l'absence de disponibilité dans leur cas est moins préjudiciable.
    - Actuellement, les membres ne sont pas tenus de se conformer à des seuils de disponibilité prescrits par des exigences réglementaires.
- Pour l'identification des risques, les fournisseurs de services de paiement préfèrent une approche réglementaire fondée sur des principes. Ce type d'approche convient mieux à la nature changeante du risque opérationnel et aux différences entre les fournisseurs de services de paiement.
    - Les participants ont indiqué que le risque associé au tiers et la fraude sont des risques importants pour leur filière, en plus des risques présentés dans le guide de discussion.
- La plupart des participants effectuent une évaluation de la criticité des actifs.
    - Il serait utile d'en savoir plus sur les façons de jauger la criticité vu que différents actifs peuvent être jugés essentiels sous différents angles (certains actifs sont considérés comme essentiels pour la continuité des opérations, alors que d'autres le sont sur le plan de la cybersécurité).
- Les fournisseurs de services de paiement privilégient, pour guider les investissements dans les mesures d'atténuation des risques, une approche globale fondée sur les risques applicable aux mesures de protection, de détection et d'intervention. Les fournisseurs examinent le risque dans sa globalité pour déterminer où résident les plus grandes vulnérabilités (celles qui ont le plus d'impact sur les clients) puis exercent des mesures de contrôle pour limiter ce risque.
    - Les mesures de contrôle des actifs ou services essentiels reçoivent plus d'investissements. Il s'agit des actifs et services dont l'absence aurait un effet négatif sur les clients.
    - Les accréditations (p. ex., normes de sécurité de l'industrie des cartes de paiement) peuvent induire des investissements dans les mesures de protection et sont exigées par des partenaires ou clients dans les clauses des contrats.
- Protection des données pendant qu'elles sont stockées, utilisées ou transmises :
    - Les participants soulignent que des protocoles précis sont en place pour protéger les données quand elles sont transmises (p. ex., cryptage).
    - Les responsabilités et obligations sont précisées dans les contrats lorsque plusieurs parties existent.
    - Les contrats que les participants concluent avec des tiers prévoient habituellement des mécanismes de surveillance.
    - Les participants ont indiqué que les lois fédérales et provinciales sur la protection des données les obligent à mettre en place des mesures de sauvegarde des données.

- Certains des participants ont expliqué que l'approche qu'ils ont adoptée pour la continuité des opérations est plus axée sur les conditions à remplir pour un retour à la normale que sur la préparation de scénarios détaillés de situations qui causeraient une rupture de service. Les mises en situation sont, cependant, très utiles pour trouver des lacunes dans les plans de continuité des opérations. De ce point de vue, les participants font régulièrement des exercices de simulation.
    - Certains participants ont indiqué que leur plan de continuité des opérations est complété par un plan plus stratégique de gestion des crises.
    - La mise à l'essai coordonnée des plans de continuité des opérations par les fournisseurs de services de paiement n'est pas une pratique courante.
- Les participants peuvent être amenés à faire des compromis entre la restauration de l'intégrité des données, de leur confidentialité, et la préservation de la disponibilité des services après un incident de nature opérationnelle. Selon les circonstances, la priorité est accordée à l'une ou à l'autre considération. Quoi qu'il en soit, le maintien ou la restauration de l'intégrité et de la confidentialité des données est la priorité aux yeux des participants.
- La dotation (fonds et personnel) des plans de continuité des opérations est habituellement intégrée aux budgets normaux de fonctionnement.
    - Les participants ont indiqué faire appel à une expertise externe pour certains types d'incidents (p. ex., cyberattaques).
    - Les participants ne pensent pas qu'il soit difficile d'avoir accès à ce genre d'expertise externe en cas d'incident, mais cela peut ne pas être vrai pour les fournisseurs de petite taille.

Les prochaines étapes

- La Banque du Canada continuera d'appuyer Finances Canada dans l'élaboration de solutions visant la gestion du risque opérationnel en vertu du cadre proposé de surveillance des paiements de détail.
- Des idées concrètes sur le risque opérationnel seront soumises aux membres afin de poursuivre la discussion lors d'une autre réunion du Comité consultatif intérimaire sur les paiements de détail.