BANQUE DU CANADA
BANK OF CANADA

La déclaration des incidents

Type de publication : ligne directrice

En vertu de la *Loi sur les activités associées aux paiements de détail* (LAAPD), si un fournisseur de services de paiement (FSP) qui exécute des activités associées aux paiements de détail prend connaissance d'un incident ayant des répercussions importantes sur un utilisateur final, un autre FSP ou une chambre de compensation d'un système de compensation et de règlement, il doit aviser sans délai la personne physique ou l'entité concernée ainsi que la Banque du Canada. La présente ligne directrice explique les exigences en matière de déclaration d'incidents et précise, s'il y a lieu, la manière dont les FSP doivent se conformer à ces exigences réglementaires selon la Banque.

Pour en savoir plus sur les termes entourant la supervision des paiements de détail, consultez le glossaire.

1. Contexte

1.1. Comme le prévoient le *Règlement sur les activités associées aux paiements de détail* et la ligne directrice *Le risque opérationnel et la réponse aux incidents*, les FSP doivent prendre des mesures immédiates pour répondre aux incidents. Tous les incidents, quelles que soient leurs répercussions, doivent faire l'objet d'une enquête, d'une réponse et d'une consignation écrite.

1.2. En vertu du sous-alinéa 5(1)i)(iii) du *Règlement*, dès qu'il a connaissance d'un incident, le FSP doit immédiatement mener une enquête. Dans le cadre de l'enquête, il doit déterminer les répercussions possibles ou avérées de l'incident sur les utilisateurs finaux, les autres FSP et les chambres de compensation.

1.3. Si le FSP prend connaissance d'un incident ayant des répercussions importantes sur un utilisateur final, un autre FSP ou une chambre de compensation d'un système de compensation et de règlement, aux termes de l'article 18 de la LAAPD, il est tenu d'aviser sans délai la Banque ainsi que les utilisateurs finaux, les autres FSP et les chambres de compensation concernés.

- Le terme « utilisateur final », aux termes de l'article 2 de la LAAPD, désigne une personne physique ou entité qui utilise un service de paiement en qualité de payeur ou de bénéficiaire.Le terme « FSP » désigne tout FSP, que la LAAPD s'applique ou non à cette personne physique ou entité. Voir la politique *Les critères d'enregistrement des fournisseurs de services de paiement*.
- Le terme « chambre de compensation » désigne une chambre de compensation d'un système de compensation et de règlement, aux termes de l'article 2 de la *Loi sur la compensation et le règlement des paiements*, qui est désigné en vertu du paragraphe 4(1) de cette loi. Voir le site Web de la Banque pour de plus amples informations sur les infrastructures de marchés financiers (IMF) désignées.

1.4. Les incidents qui n'ont pas de répercussions importantes sur les personnes physiques ou les entités mentionnées à l'article 1.2 de la présente ligne directrice ne sont pas visés par les exigences de déclaration

prévues à l'article 18 de la LAAPD. Toutefois, la Banque peut demander séparément des renseignements sur ces incidents afin d'évaluer si un FSP se conforme à l'article 18 de la LAAPD et à ses obligations de gestion des risques opérationnels prévues par l'article 17 de la LAAPD.

2. Incidents liés aux FSP

2.1. L'article 2 de la LAAPD définit le terme « incident » de la façon suivante : « Événement ou série d'événements liés qui sont non planifiés par le [FSP] et qui entravent, perturbent ou interrompent – ou qui pourraient vraisemblablement entraver, perturber ou interrompre – une activité associée aux paiements de détail exécutée par le [FSP]. »

2.1.1. Au sens de cette définition, la Banque considère que les événements « entravent, perturbent ou interrompent » une activité notamment lorsqu'ils ont des conséquences négatives sur la confidentialité, l'intégrité ou la disponibilité :

- des activités associées aux paiements de détail d'un FSP
- des systèmes, données et renseignements engagés dans l'exécution de ces activités par le FSP

2.1.2. Comme indiqué dans la ligne directrice *Le risque opérationnel et la réponse aux incidents* :

- l'intégrité fait référence à l'exactitude et à la complétude, soit l'absence de modification ou de destruction indue d'un système, de données ou de renseignements
- la confidentialité est la propriété selon laquelle une donnée ou une information n'est pas diffusée ni divulguée à des personnes physiques, entités, processus ou systèmes non autorisés, soit la préservation des restrictions autorisées entourant l'accessibilité et la divulgation des données et des renseignements
- la disponibilité est la propriété d'un service accessible et utilisable à la demande par une entité autorisée, soit la possibilité d'accès et de recours fiable et opportun à un service de paiement, à un système, à des données ou à des renseignements

2.1.3. Les incidents peuvent comprendre des événements subis ou détectés par les mandataires ou les tiers fournisseurs de services du FSP. Les FSP sont tenus de déclarer les incidents ayant des répercussions importantes subis ou détectés par leurs mandataires ou tiers fournisseurs de services.

3. Incidents ayant des répercussions importantes

3.1. Seuls les incidents ayant des répercussions importantes sur un utilisateur final, un FSP ou une chambre de compensation sont visés par l'obligation de déclaration prévue à l'article 18 de la LAAPD. Cette obligation concerne les incidents qui touchent au moins une de ces parties de manière importante. Pour déterminer si un incident a des répercussions importantes sur un utilisateur final, un FSP ou une chambre de compensation, le FSP doit évaluer ses circonstances particulières, son modèle d'affaires, la nature des services précis qu'il offre et d'autres facteurs pertinents.

Les paragraphes qui suivent présentent des exemples d'incidents pouvant avoir des répercussions importantes sur un utilisateur final, un FSP ou une chambre de compensation d'un système de compensation et de règlement désigné, et de circonstances qui pourraient les provoquer.

Ces exemples ne sont pas exhaustifs; il pourrait y avoir d'autres incidents qui, même s'ils ne figurent pas ici, pourraient être considérés comme ayant des répercussions importantes selon la LAAPD. Le FSP doit user de son jugement pour déterminer si un incident aura des répercussions importantes sur un utilisateur final, un autre FSP ou une chambre de compensation, puisque ce ne sera pas toujours le cas.

3.1.1. Les fonds d'un utilisateur final détenus par un FSP, quel qu'en soit le montant, ont été perdus irrémédiablement ou deviennent indisponibles en permanence avant que l'utilisateur final puisse les retirer ou les transférer à une autre personne physique ou entité. Voici quelques exemples d'incidents susceptibles d'avoir de telles répercussions :

- les fonds d'un utilisateur final sont perdus à cause de défaillances opérationnelles dans les processus ou les systèmes du FSP, notamment un vol ou une lacune de système résultant d'une négligence ou d'un manquement du FSP, ce qui exclut les pertes attribuables à un geste de l'utilisateur final, comme dans le cas d'une fraude autorisée
- le fournisseur de compte qui détient les fonds de l'utilisateur final a cessé ses activités ou éprouve des difficultés financières, ce qui rend les fonds de l'utilisateur final irrécupérables ou inaccessibles par celui-ci, en tout ou en partie

3.1.2. Le FSP subit une interruption ayant des répercussions importantes sur la disponibilité de ses activités associées aux paiements de détail. Il est question d'une interruption lorsque les tâches, processus ou systèmes entourant les activités associées aux paiements de détail d'un FSP sont suspendus, ce qui empêche la prestation de ces activités auprès d'un ou de plusieurs utilisateurs finaux (p. ex., comptes de paiement inaccessible) ou touche un autre FSP ou une chambre de compensation. La Banque s'attend à ce que le FSP évalue ses circonstances particulières, son modèle d'affaires, la nature des services précis qu'il offre et d'autres facteurs pertinents pour déterminer à quel moment une interruption devient importante. Voici quelques exemples de causes d'incidents susceptibles d'avoir des répercussions importantes :

- défaillance technologique
- perte du centre de données
- perte du service hébergeant l'infrastructure
- perte d'un tiers
- cyberattaque

3.1.3. Le FSP fait l'objet d'une procédure d'insolvabilité aux termes du paragraphe 14(3) du *Règlement*.

3.1.4. Les renseignements confidentiels d'un utilisateur final, d'un FSP ou d'une chambre de compensation sont consultés ou communiqués sans autorisation, ce qui entraîne ou crée un risque réel de tort important pour l'utilisateur final, le FSP ou la chambre de compensation. Voici quelques exemples de torts importants :

- lésions corporelles
- humiliation
- atteinte à la réputation ou aux relations
- perte d'emploi, d'affaires ou de possibilités professionnelles
- perte financière
- vol d'identité
- effets négatifs sur le dossier de crédit
- dommages matériels ou perte de biens

Le FSP doit évaluer le risque de tort important qui pourrait résulter d'une atteinte à la confidentialité de toute donnée ou de tout renseignement qu'il juge confidentiel. Il s'agit notamment des renseignements de nature personnelle, financière ou juridique et des autres informations de clients concernant des utilisateurs finaux, d'autres FSP et des chambres de compensation, ainsi que de toute information devant rester confidentielle au sujet des activités associées aux paiements de détail du FSP. Pour déterminer si une atteinte à la confidentialité (c.-à-d. la consultation ou la communication non autorisée de renseignements confidentiels) entraîne ou crée un risque réel de tort important pour un utilisateur final, un FSP ou une chambre de compensation, le FSP doit évaluer les éléments suivants :

- le caractère sensible des renseignements atteints
- la probabilité que ces renseignements aient été, soient ou seront utilisés à mauvais escient

3.1.5. L'intégrité des activités associées aux paiements de détail du FSP est compromise d'une façon qui entraîne des répercussions importantes sur un utilisateur final, un FSP ou une chambre de compensation. Voici quelques exemples d'incidents susceptibles d'avoir de telles répercussions :

- compromission du registre du FSP (comme décrit dans la ligne directrice *La protection des fonds des utilisateurs finaux*)
- compromission des relevés d'opérations
- erreurs de traitement des opérations faisant qu'un bénéficiaire reçoit un montant différent de celui attendu (p. ex., le payeur envoie X $, mais le bénéficiaire reçoit Y $)
- mauvais acheminement des fonds d'un utilisateur final (c.-à-d. que les fonds ne sont pas déposés dans le compte de l'utilisateur final comme prévu)
- détournement d'instructions relatives à un transfert électronique de fonds
- calcul incorrect à l'étape de la compensation ou du règlement
- modification ou suppression non autorisée d'autres données ou informations

3.1.6. Un incident pourrait avoir des répercussions importantes de plusieurs manières, c'est-à-dire lorsque plus d'un des seuils définis dans les exemples de la section 3 est atteint. Autrement dit, les seuils d'importance peuvent se chevaucher (p. ex., un incident compromet l'intégrité du registre d'un FSP, ce qui entraîne la perte des fonds d'un utilisateur final).

4. Déclaration des incidents

4.1. Les incidents ayant des répercussions importantes doivent être déclarés à l'utilisateur final, au FSP ou à la chambre de compensation concerné, ainsi qu'à la Banque, sans délai et au plus tard 48 heures après que le FSP détermine que l'incident est important .

4.1.1. Si un incident n'atteint pas les seuils d'importance indiqués dans les exemples de la section 3 de la présente ligne directrice lorsqu'il est détecté pour la première fois, mais que son importance augmente au fil du temps, il doit être déclaré sans délai et au plus tard dans les 48 heures suivant le moment où on détermine qu'il s'agit d'un incident important.

Déclaration des incidents à la Banque du Canada

4.2. Tout incident ayant des répercussions importantes sur un utilisateur final, un FSP ou une chambre de compensation doit être déclaré à la Banque à l'aide des modèles d'avis d'incident accessibles dans Connexion FSP.

Dans Connexion FSP, les FSP peuvent fournir à la Banque des avis successifs selon les besoins, notamment un avis initial, un avis intermédiaire et un avis définitif.

- Avis initial : Pour chaque incident important, le FSP est tenu de fournir un avis initial sans délai, au plus tard 48 heures après avoir déterminé que l'incident est important.
- Avis intermédiaire : Un avis intermédiaire doit être fourni à la Banque si l'incident a évolué de façon importante et lorsque de nouvelles informations pertinentes sont disponibles.
- Avis définitif : Un avis définitif doit être fourni lorsque tous les détails de l'incident ont été établis, notamment par l'analyse de la cause première, et que l'incident a été résolu.
- Il faut envoyer un avis initial et un avis définitif pour tous les incidents importants. Cela dit, si l'incident est résolu et que toute l'information exigée est disponible au moment de l'avis initial (c.-à-d. dans les 48 heures après avoir déterminé que l'incident est important), le FSP peut fournir un seul avis qui contient toute l'information pertinente (et qui sert aussi d'avis définitif).

La Banque s'attend à ce que le FSP fournisse ses avis d'incident dans Connexion FSP. Cependant, dans des circonstances exceptionnelles, par exemple si les capacités techniques du FSP sont considérablement réduites et qu'il lui est impossible de fournir ces avis en ligne, il peut les fournir par téléphone au numéro indiqué sur le site Web de la Banque.

4.3. Conformément à l'article 11 du *Règlement*, l'avis d'incident transmis à la Banque par le FSP doit contenir les informations suivantes.

4.3.1. Les coordonnées du FSP, y compris :

- son nom
- le numéro de téléphone et l'adresse électronique d'une personne-ressource qui serait en mesure d'éclairer la Banque au sujet de l'incident, si celle-ci l'exige

4.3.2. Une description de l'incident et de ses répercussions importantes sur les utilisateurs finaux, les FSP ou les chambres de compensation. La description doit comprendre :

- la date et l'heure du début de l'incident
- la date et l'heure de la détection de l'incident
- si elles diffèrent de la date et de l'heure de la détection, la date et l'heure auxquelles il a été déterminé que l'incident est devenu important, selon les exemples à la section 3 de la présente ligne directrice
- la date et l'heure de la résolution (fin) de l'incident
- la manière dont l'incident a été détecté (p. ex., avis d'un utilisateur final ou détection par le FSP ou un tiers fournisseur de services)
- une brève description de l'incident, notamment du problème précis, ainsi que des activités associées aux paiements de détail qui ont été touchées et en quoi elles l'ont été

- des précisions sur la nature des répercussions réelles ou estimées de l'incident sur les utilisateurs finaux, les autres FSP ou les chambres de compensation (p. ex., le nombre de personnes physiques ou d'entités touchées)
- les répercussions possibles ou avérées de l'incident sur les systèmes, données et renseignements engagés dans l'exécution des activités associées aux paiements de détail

4.3.3. Les mesures prises à ce jour en réponse à l'incident (p. ex., transmission aux échelons supérieurs).

4.3.4. Les précisions concernant la cause première de l'incident et son analyse.

4.4. La Banque peut exiger qu'un FSP produise un avis de suivi, comme l'autorise le paragraphe 19(1) de la LAAPD, si elle estime que des informations supplémentaires sur un incident sont nécessaires ou doivent être communiquées à d'autres personnes physiques ou entités[1].

4.4.1. Dans ces cas, l'arrêté imposant l'avis de suivi indique à qui cet avis doit être donné (p. ex., la Banque, tous les utilisateurs finaux ou certains utilisateurs finaux), quand et comment cet avis doit être donné, et quels renseignements sont requis dans cet avis au moment où la Banque prend l'arrêté.

4.4.2. Le contenu de l'avis de suivi dépend de l'incident en question, car il doit refléter les circonstances individuelles de l'incident.

4.4.3. Un FSP peut être tenu d'envoyer plusieurs avis de suivi aux personnes physiques ou entités ayant subi des répercussions importantes, si cela est jugé nécessaire, jusqu'à ce que tous les détails pertinents concernant l'incident aient été fournis.

Déclaration des incidents aux utilisateurs finaux, aux FSP et aux chambres de compensation concernés ayant subi des répercussions importantes

4.5. En vertu de l'article 12 du *Règlement*, le FSP est tenu d'aviser tous les utilisateurs finaux, les FSP et les chambres de compensation ayant subi des répercussions importantes.

- Si un utilisateur final, un FSP ou une chambre de compensation ayant subi des répercussions importantes a fourni des coordonnées au FSP, ce dernier doit aviser la personne physique ou l'entité concernée en utilisant ses coordonnées les plus récentes.
- Si le FSP ne dispose pas des coordonnées de chaque utilisateur final, FSP ou chambre de compensation ayant subi des répercussions importantes, il est tenu de publier un avis sur son site Web.
- Pour faciliter la déclaration des incidents dans les meilleurs délais, on recommande aux FSP de tenir à jour les coordonnées de leurs utilisateurs finaux ainsi que celles des FSP et des chambres de compensation avec qui ils entretiennent des liens.

4.5.1. Par souci de clarté, lorsqu'un incident survenu chez un FSP a des répercussions importantes sur un autre FSP qui effectue des activités associées aux paiements de détail, le FSP touché est tenu d'aviser ses propres utilisateurs finaux s'ils ont subi des répercussions importantes. Voici un exemple :

---

1 La Banque peut également demander des renseignements supplémentaires en soumettant une demande de renseignements aux termes du paragraphe 65(1) de la LAAPD. Le paragraphe 43(2) du *Règlement* accorde au FSP un délai de réponse de 24 heures si les renseignements que la Banque lui demande sont liés à un incident qui se poursuit et qui pourrait avoir des conséquences négatives importantes sur un utilisateur final, un FSP (assujetti ou non à la LAAPD) ou une chambre de compensation d'un système de compensation et de règlement que la Banque surveille en vertu de la *Loi sur la compensation et le règlement des paiements*.

- Si le FSP A subit un incident qui a des répercussions importantes à la fois sur ses utilisateurs finaux et sur le FSP B, le FSP A est tenu d'aviser tous ses utilisateurs finaux touchés ainsi que le FSP B.
- Ensuite, le FSP B est tenu d'aviser ses utilisateurs finaux ayant subi les répercussions importantes de l'incident, si cet incident répond effectivement aux critères qu'il utilise pour reconnaître un incident important.

4.6. Les avis du FSP concernant un incident doivent être envoyés sans délai aux coordonnées disponibles de chaque utilisateur final, FSP ou chambre de compensation ayant subi des répercussions importantes, au plus tard 48 heures après que le FSP détermine que l'incident est important.

4.6.1. La Banque s'attend à ce que ces avis soient transmis directement à l'utilisateur final, au FSP ou à la chambre de compensation concerné.

4.6.2. Par exemple, la transmission de ces avis par courriel, par message texte ou sur l'application ou le site Web du FSP (dans les cas où le FSP ne dispose pas des coordonnées de l'utilisateur final, du FSP ou de la chambre de compensation concerné) serait appropriée, tandis que leur publication sur les médias sociaux ne serait pas considérée comme un avis approprié.

4.6.3. Toutefois, si le FSP souhaite publier un avis d'incident sur les médias sociaux en plus d'envoyer un courriel à un utilisateur final, par exemple, les attentes de la Banque ne l'empêchent pas de le faire.

4.6.4. Si le FSP a un motif de croire que le fait d'aviser les utilisateurs finaux dans les 48 heures peut augmenter le risque de tort important pour un utilisateur final ou accroître le risque de l'incident, ou que ce n'est pas faisable, il doit aviser la Banque. Le FSP doit utiliser les modèles d'avis d'incident fournis dans Connexion FSP pour préciser en quoi il ne peut pas aviser les utilisateurs finaux. La Banque s'attend à ce que de tels incidents surviennent en nombre limité et dans des situations très particulières.

4.7. Conformément à l'article 12 du *Règlement*, l'avis d'incident adressé par un FSP aux utilisateurs finaux, aux FSP et aux chambres de compensation ayant subi des répercussions importantes doit contenir les informations suivantes :

4.7.1. le nom du FSP

4.7.2. une description de l'incident et de ses répercussions sur les utilisateurs finaux, les FSP ou les chambres de compensation, notamment :

- la date et l'heure du début de l'incident
- la date de la détection de l'incident
- la date de la résolution (fin) de l'incident
- des précisions sur la nature des répercussions réelles ou estimées de l'incident sur l'utilisateur final, le FSP ou la chambre de compensation à aviser

4.7.3. les mesures correctives que peuvent prendre les personnes physiques ou entités concernées pour atténuer les effets négatifs de l'incident, le cas échéant (p. ex., changement de mot de passe)

4.8. Il convient de noter que les FSP, en tant que participants aux systèmes de compensation et de règlement, peuvent être soumis à des exigences de déclaration d'incidents tant de la part de la Banque, au titre de la

LAAPD, qu'en vertu des règles ou des dispositions contractuelles liées à la participation au système de compensation et de règlement.

Si tel est le cas, et si un FSP déclare des incidents à une chambre de compensation selon les critères établis dans le cadre des obligations de participation de la chambre, mais que ces critères sont différents de ceux établis par la Banque en vertu de la LAAPD, la chambre peut choisir de demander à un FSP de fournir des avis d'incidents selon ses propres critères uniquement ou peut choisir de recevoir à la fois les avis prévus par la LAAPD et ceux prévus par ses propres critères.

4.8.1. Dans un cas comme dans l'autre, tous les incidents importants, tels que définis dans la présente ligne directrice, doivent être déclarés à la Banque.

4.8.2. Le respect des obligations de la Banque en matière de déclaration d'incidents ne dispense pas un FSP de respecter les obligations de son adhésion à une chambre de compensation, ou toute autre obligation de déclaration.

4.9. Si un incident relève à la fois des exigences de la Banque en matière de déclaration d'incident et des lois fédérales ou provinciales sur la protection des renseignements personnels (p. ex., atteinte à la confidentialité des renseignements personnels créant un risque réel de tort important pour la personne physique ou l'entité), le FSP est toujours tenu, en vertu de la LAAPD, d'en informer la Banque et les personnes physiques ou entités ayant subi des répercussions importantes. Il est possible de n'envoyer qu'un seul avis aux utilisateurs finaux ou entités ayant subi des répercussions importantes, pourvu que cet avis respecte toutes les exigences légales et réglementaires applicables.