OBSI OMBUDSMAN FOR BANKING SERVICES AND INVESTMENTS
OSBI OMBUDSMAN DES SERVICES BANCAIRES ET D'INVESTISSEMENT

1er mai 2026

Envoyé par courriel à : consumer.consommateur@fin.gc.ca

Judith Hamel
Direction de la politique du secteur financier
Ministère des Finances Canada
Édifice James Michael Flaherty
90, rue Elgin
Ottawa (Ontario) K1A 0G5

Objet : Réponse à la consultation sur la Stratégie nationale antifraude

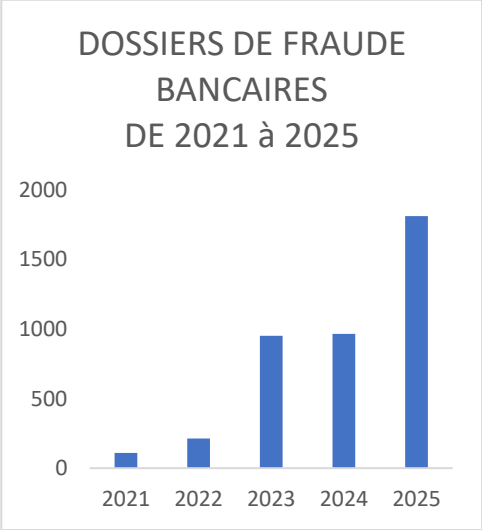
L'Ombudsman des services bancaires et d'investissement (OSBI) est heureux de soumettre ses commentaires au ministère des Finances du Canada en réponse à sa récente consultation, *Consultation sur la Stratégie nationale antifraude*.

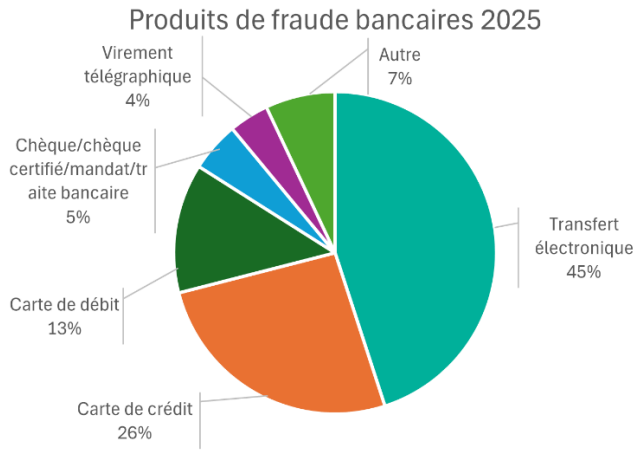
L'OSBI est un organisme national indépendant et sans but lucratif qui aide les consommateurs et plus de 1 500 firmes des secteurs des services financiers partout au Canada à régler leurs différends et à diminuer le nombre de ces conflits. Ses services sont offerts dans les deux langues officielles. Nous offrons des services aux institutions financières sous réglementation fédérale, aux maisons de courtage sous réglementation provinciale et aux coopératives de crédit de partout au pays. Nous offrons ces services depuis plus de 30 ans. À ce titre, nous sommes très bien placés pour émettre nos points de vue et proposer nos idées dans le cadre de cette importante consultation.

L'expérience d'OSBI en matière de fraude

Les cas impliquant la fraude, en particulier la fraude par virements électroniques et d'autres types de fraude numérique, ont touché un nombre sans précédent de consommateurs canadiens ces dernières années. Cela se manifeste par une augmentation spectaculaire du volume de plaintes concernant ces enjeux. Celles-ci ont été transmises par les consommateurs à l'OSBI.

En 2021, l'OSBI a ouvert 110 dossiers liés à la fraude bancaire. En 2022, ce nombre avait presque doublé pour atteindre 213 cas. Depuis 2022, nous avons constaté une augmentation continue et significative des dossiers de fraude bancaire. En 2024, nous avons ouvert 965 dossiers de fraude et en 2025, ce nombre est passé à 1 812. Nous sommes en voie d'ouvrir encore plus de dossiers de fraude bancaire en 2026.





Une partie de cette augmentation du volume de plaintes est liée aux importantes modifications apportées en 2022 au cadre de protection des consommateurs de la Loi sur les banques, qui ont réduit l'attrition des plaintes dans les banques sous réglementation fédérale, ainsi qu'à notre désignation comme organisme externe de règlement des plaintes (ECB) pour toutes les banques sous réglementation fédérale en 2025. Cependant, nous constatons que cette hausse de la fraude bancaire au Canada s'inscrit également dans une tendance mondiale. Les services d'ombudsman financier du monde entier signalent des augmentations tout aussi importantes des cas de fraude bancaire.

Questions pour la consultation

1. Les trois secteurs susmentionnés conviennent-ils pour la phase initiale d'un cadre? Faudrait-il prendre en considération d'autres secteurs?

L'OSBI convient que les trois secteurs décrits sont appropriés pour la phase initiale du cadre. Dans les dossiers que nous traitons, la fraude implique fréquemment les secteurs financier et des télécommunications, et débute souvent par des interactions sur les plateformes numériques. Les entreprises et les particuliers de ces trois secteurs sont les mieux placés pour agir en tant que gardiens et instaurer des mesures de protection pour les consommateurs canadiens.

Bien que les pertes liées à la fraude soient souvent constatées dans le secteur des services financiers, nous avons observé que de nombreux parcours frauduleux commencent à l'extérieur du secteur financier et que les secteurs des télécommunications et des plateformes numériques sont régulièrement exploités par les fraudeurs. Ces secteurs ont des possibilités évidentes de réduire ou de prévenir les fraudes grâce à des interventions précoces, par exemple en empêchant la falsification de l'identité de l'appelant ou en détectant et en interrompant les sollicitations frauduleuses sur des plateformes numériques. D'autres secteurs potentiels qui pourraient être envisagés pour les prochaines phases du cadre comprennent les fournisseurs de cartes de crédit, Interac, les plateformes de négociation de cryptomonnaies et d'autres intermédiaires de paiement.

Pour résoudre le problème de la fraude généralisée qui touche les consommateurs au Canada, des efforts coordonnés de la part de plusieurs gardiens dans les trois secteurs déterminés seront nécessaires. Bien qu'aucune intervention ne soit efficace à 100 % pour lutter contre la fraude, chaque secteur, en mettant à profit sa position et ses outils uniques pour prévenir, détecter et interrompre certaines fraudes, ces actions, collectivement, offrent un potentiel significatif pour aider à protéger les consommateurs canadiens contre le risque d'être victimes de fraudes.

2. Quel rôle un organisme de réglementation central pourrait-il jouer en ce qui concerne un cadre multisectoriel de lutte contre la fraude?

L'OSBI soutient la mise en place d'un organisme central robuste pour coordonner les efforts de lutte contre la fraude entre les secteurs et centraliser la collecte et le partage de l'information. Un organisme central pourrait :

- établir des définitions communes pour les différents types de fraude et de préjudice aux consommateurs afin d'assurer une communication efficace et la collecte de données
- Développer des exigences de déclaration uniformes
- Agréger des données provenant de plusieurs secteurs et les analyser pour identifier les tendances, les menaces émergentes et les opportunités de prévention.
- établir des attentes complémentaires pour chaque secteur, fondées sur les menaces de fraude les plus récentes et émergentes, et collaborer avec les organismes de réglementation sectoriels pour assurer le suivi de la conformité à ces attentes
- Jouer un rôle de coordination lors d'incidents majeurs de fraude
- favoriser un partage sécurisé et structuré de l'information entre les régulateurs sectoriels et les forces de l'ordre, afin que les organisations puissent utiliser des indicateurs fiables et des aperçus à l'échelle du système pour prévenir, détecter et contrer les fraudes

3. Quel rôle les organismes de réglementation sectoriels pourraient-ils jouer en ce qui concerne le cadre?

Les régulateurs sectoriels sont les mieux placés pour traduire les attentes du Cadre en lignes directrices ou exigences opérationnelles claires, adaptées aux produits, canaux et risques dans leurs secteurs respectifs. Ces organismes de réglementation sont mieux placés pour superviser la conformité grâce aux outils existants (p. ex., directives, examens de conformité et application de la loi).

Des attentes cohérentes à l'échelle du secteur sont importantes pour réduire la variabilité des pratiques et des résultats des entreprises, ce que les consommateurs pourraient percevoir comme une injustice s'ils sont exposés à des niveaux de protection contre la fraude différents selon l'endroit où la transaction a lieu.

4. Comment peut-on assurer une surveillance efficace du cadre, sans chevauchement de la surveillance existante des trois secteurs?

Il est important de reconnaître qu'il existe actuellement très peu de supervision des comportements de marché spécifiques à la fraude dans les secteurs qui seront soumis au nouveau Cadre. Cela offre au nouveau régulateur l'occasion de collaborer avec les organismes de réglementation existants afin de développer un cadre cohérent de détection, de prévention et de perturbation de la fraude, au bénéfice de tous les Canadiens, tout en réduisant le risque de duplication.

Une surveillance efficace des activités anti-fraude dans les trois secteurs peut être assurée en distinguant entre l'élaboration de stratégies, l'établissement de normes et les activités de coordination, qui devraient relever du nouveau régulateur, et la supervision et l'application sectorielles, qui devraient relever des

régulateurs existants. Bien qu'une certaine duplication d'efforts puisse être inévitable, du point de vue de la protection des consommateurs, éviter les lacunes de responsabilité, surtout pour les fraudes impliquant plusieurs secteurs, est plus important que de minimiser le chevauchement administratif.

5. À quel moment les organismes de réglementation du cadre devraient-ils être autorisés à communiquer à un autre organisme de réglementation des informations sur l'activité frauduleuse afin de contribuer à la réalisation des objectifs de la stratégie qui consistent à prévenir, à détecter et à perturber les activités frauduleuses et à mener des enquêtes à cet égard?

Compte tenu de l'objectif global du Cadre et de l'importance vitale de lutter contre la fraude au Canada, une approche large et ouverte du partage de l'information est justifiée. Bien que les renseignements personnels doivent toujours être protégés et que tous les participants du Cadre doivent collectivement respecter des exigences appropriées en matière de protection des données, un partage ouvert de l'information entre les participants du Cadre serait bénéfique pour l'atteinte des objectifs généraux de l'initiative.

Les informations partagées ouvertement permettraient aux organismes de réglementation d'identifier des campagnes ou activités frauduleuses actives, des schémas affectant plus d'un secteur, une défaillance systémique dans les contrôles de fraude et de protection des consommateurs d'une entreprise ou d'un secteur, ou de nouvelles méthodes de fraude susceptibles de se propager rapidement. Le nouveau régulateur antifraude devrait établir des protocoles pour ce partage d'informations et pourrait agir comme un centre de dépôt pour les informations partagées.

Dans le contexte d'une large autorité de partage d'informations aux fins du Cadre, il conviendrait de mettre davantage l'accent sur l'identification des circonstances où le partage d'informations devrait être interdit.

6. Le cas échéant, quelles sont précisément les informations qui devraient être communiquées et dans quelles circonstances et à quelles fins précises devraient-elles l'être?

Les autorités de régulation devraient partager des informations utiles qui permettent de repérer et de combattre la fraude. Cela pourrait inclure les types et tendances de fraude, les faiblesses des contrôles internes et des signes avant-coureurs spécifiques, tels que des sites web ou des numéros de téléphone frauduleux confirmés, ainsi que des réseaux ou des modes opératoires connus.

L'information devrait être partagée lorsqu'il existe des preuves de schémas de fraude actifs ou émergents touchant plus d'une entreprise ou d'un secteur, ou de défaillances répétées dans les contrôles permettant à la fraude de se poursuivre.

L'objectif doit être celui décrit précédemment dans la stratégie : prévenir la fraude, améliorer la détection, perturber les arnaques actives, réduire les préjudices aux consommateurs.

7. Quels mécanismes de protection de la vie privée ou de surveillance faudrait-il mettre en place pour de telles initiatives d'échange d'information?

Bien que nous appuyions le partage étendu des renseignements entre les organismes de réglementation, selon notre expérience, les renseignements personnels sont généralement non pertinents aux objectifs mentionnés ci-dessus et ne devraient être inclus que si nécessaire.

Les renseignements personnels permettant d'identifier directement les victimes de fraude ou les consommateurs de manière plus générale ne devraient être partagés que dans des cas exceptionnels où cela est strictement nécessaire pour prévenir un préjudice imminent ou soutenir une enquête, et exclusivement aux fins de prévention, de détection, de perturbation et d'enquête.

Une exception claire à cela concerne l'identification d'acteurs frauduleux connus ou présumés. De toute évidence, le partage de ces identités est pertinent pour la prévention et l'interruption des fraudes et devrait être permis; cependant, il présente également le risque de causer un préjudice grave à toute personne ou entité faussement identifiée comme acteur ou facilitateur frauduleux. Les conséquences d'une identification erronée comme acteur frauduleux pourraient inclure le gel des comptes, la perte de fonds en transit et une perturbation générale de toutes les interactions financières, causant potentiellement un préjudice financier important. Pour cette raison, un processus clair devrait être disponible pour toutes les personnes ou entités identifiées afin de contester et d'annuler toute identification de ce type et de rétablir leurs services financiers précédemment disponibles.

8. Quand les organismes de réglementation du cadre devraient-ils être autorisés à communiquer des informations sur les activités frauduleuses aux organismes d'application de la loi aux fins de prévention, de détection et de perturbation des fraudes, et d'enquête sur celles-ci?

9. Quand [les organismes d'application de la loi] devraient-ils être autorisés à communiquer des informations sur les activités frauduleuses à des organisations du secteur privé?

10. Le cas échéant, quelles sont précisément les informations qui devraient être communiquées et dans quelles circonstances et à quelles fins précises devraient-elles l'être?

11. Quels mécanismes de protection de la vie privée ou de surveillance faudrait-il mettre en place pour de telles initiatives d'échange d'information?

Réponse aux questions 8 à 11

Nos points de vue sur le partage d'informations entre les organismes d'application de la loi et les régulateurs du Cadre sont similaires à ceux énoncés plus haut concernant le partage d'informations entre régulateurs. De façon générale, nous constatons que le partage accru de l'information favorise et s'aligne sur les objectifs globaux du Cadre, sous réserve de limitations concernant le partage de renseignements personnels et de prudence quant aux conséquences potentiellement négatives d'une identification inexacte d'une personne ou d'une entité comme auteur de fraude. Tout partage de ce type devrait être encadré de manière à prévenir tout dommage non intentionnel et inclure des garanties afin que les

consommateurs puissent exercer un recours ou contester les décisions fondées sur les informations partagées.

Nous notons également que, du point de vue du préjudice aux consommateurs, le renvoi aux forces de l'ordre ne devrait pas remplacer ou retarder les mesures actives de protection des consommateurs par les organisations (p. ex., blocage de transactions, avertissements ou tentatives de rappel).

De même, le partage d'informations avec des entreprises du secteur privé, que ce soit par les agences d'application de la loi ou par l'organisme de réglementation du Cadre, pourrait permettre de perturber et d'empêcher de manière significative des fraudes en cours, mais présente également le risque de causer un préjudice grave à toute personne identifiée à tort. D'après notre expérience, les institutions financières ont une grande aversion au risque et sont susceptibles de refuser d'offrir des services à toute personne qu'elles considèrent comme potentiellement impliquée dans un crime ou un acte répréhensible, ce qui peut entraîner des dommages importants pour la personne concernée. Comme décrit ci-dessus, les personnes identifiées devraient être informées qu'elles ont été identifiées et se voir offrir la possibilité de répondre et/ou de contester les allégations portées contre elles.

12. Comment les organisations devraient-elles être tenues d'intégrer la conformité au cadre dans leur modèle de gouvernance?

Il existe de nombreuses façons pour les organisations d'intégrer la conformité au Cadre dans leurs modèles de gouvernance, notamment la supervision au niveau du conseil d'administration, l'attribution claire de la responsabilité aux cadres, la documentation des évaluations des risques de fraude, les tests et l'assurance des contrôles, les protocoles d'escalade, ainsi que la remédiation post-incident avec leçons tirées de l'expérience.

13. Comment les organisations peuvent-elles s'assurer que la formation sur la lutte contre la fraude est efficace, et comment cela devrait-il être pris en considération dans les politiques ou les lois du gouvernement?

Il est primordial que le personnel de première ligne soit habilité à intervenir lorsqu'il y a des signes qu'un consommateur pourrait être exposé à un risque de fraude. Le personnel des succursales et des centres d'appels est souvent le mieux placé pour détecter les fraudes typiques, avertir les consommateurs en temps réel et agir immédiatement afin d'éviter d'autres préjudices, notamment en imposant des gels temporaires si la situation l'exige. Pour soutenir ce rôle, il conviendrait d'envisager des protections de type zone sûre qui permettent au personnel d'agir de bonne foi pour protéger les consommateurs, sans craindre des conséquences négatives pour eux-mêmes ou leur institution.

La formation anti-fraude devrait être axée sur les rôles, orientée par des scénarios, continuellement mise à jour et évaluée en fonction de la compétence plutôt que de la présence. La formation anti-fraude devrait être spécifique au rôle. La formation devrait être renouvelée à mesure que les typologies de fraude évoluent et devrait inclure le personnel de première ligne, l'équipe chargée de la fraude, les gestionnaires de plaintes et la direction. Le régulateur du cadre pourrait exiger une évaluation périodique de l'efficacité de la formation, en utilisant à la fois des tests et des mesures de résultats.

14. Quand et comment les organisations devraient-elles être tenues de vérifier l'identité des utilisateurs de leurs services?

Les organisations devraient être tenues de valider l'identité avant de traiter des changements de compte, de recevoir des instructions et de divulguer des renseignements. Les pratiques d'identification qui peuvent être plus facilement exploitées par des fraudeurs comprennent l'authentification à deux facteurs par SMS et la dépendance excessive à des informations personnelles de base, qui peuvent être largement accessibles en raison des violations de données et de l'exposition en ligne. D'après notre expérience, les méthodes d'identification plus solides comprennent l'identification biométrique, des informations uniques sur l'utilisateur, telles que les adresses IP et les comportements, ainsi que l'utilisation d'informations difficiles à obtenir ou à deviner pour les fraudeurs, comme des détails issus de l'activité récente des comptes (p. ex., le dernier paiement effectué).

Les organisations devraient adopter une approche axée sur le risque pour la validation de l'identité, avec des méthodes de vérification plus strictes pour les actions à risque élevé, telles que la récupération de compte, les modifications d'identifiants ou de coordonnées, l'ajout de nouveaux bénéficiaires et les transferts exceptionnellement importants ou atypiques. Dans de nombreuses plaintes liées à la fraude, la compromission survient à ces moments critiques. Des attentes claires concernant la validation de l'identité aident aussi à déterminer si des mesures raisonnables ont été prises lorsque des pertes surviennent.

15. Quelles informations sur la fraude les organisations devraient-elles être tenues de mettre à la disposition des personnes qui utilisent ou pourraient utiliser leurs services?

Des informations sur la fraude claires et faciles à comprendre devraient être accessibles aux consommateurs, surtout dans les moments clés qui précèdent l'envoi de l'argent. Cela comprend des avertissements clairs pour les transactions à plus haut-risque, des explications des arnaques courantes, des mesures que les consommateurs devraient suivre pour conserver des registres, ainsi que des informations simples sur la façon de signaler une fraude suspectée et sur ce qui se passera ensuite. D'après notre expérience, les avertissements généraux publiés sur des sites web, envoyés par courriels non sollicités ou cachés dans des contrats sont peu susceptibles d'influencer les actions des gens et ne répondent pas aux attentes des consommateurs en matière de véritable protection.

16. Comment devrait-on évaluer l'efficacité des activités de sensibilisation des organisations en matière de fraude pour s'assurer qu'elles permettent de réduire de manière appréciable les préjudices?

L'efficacité pourrait être mesurée par l'analyse des données de fraude signalées, telles que la réduction de la victimisation répétée, la diminution des pertes évitables causées par des arnaques courantes ou graves, et des preuves d'une meilleure compréhension des consommateurs grâce à des tests ou des enquêtes. Les tendances des plaintes, notamment la confusion persistante concernant les protections et le fonctionnement des processus, devraient également être prises en compte dans l'évaluation. L'OSBI soutient la communication des résultats des programmes éducatifs avec les organismes de réglementation afin que ces programmes puissent être améliorés sur la base de preuves plutôt que d'hypothèses.

17. Quelles règles sectorielles de prévention de la fraude faudrait-il mettre en place?

Secteur des services financiers

Dans notre réponse à la consultation du ministère des Finances sur les propositions visant à renforcer le secteur financier canadien en septembre 2024, nous avons présenté en détail notre expérience et nos points de vue sur trois initiatives politiques potentielles étroitement liées pour aborder la fraude dans le secteur des services financiers. Les thèmes de ce commentaire étaient les suivants :

- Exiger des banques qu'elles détectent la fraude
- Exiger des banques qu'elles retardent ou empêchent les transactions
- Introduire un seuil de responsabilité maximal pour les titulaires de compte qui sont victimes de fraude bancaire, ce qui fait passer la responsabilité des transactions frauduleuses des consommateurs aux banques

Notre position sur ces importantes initiatives de politique publique demeure inchangée. Nous notons que certaines interventions politiques discutées lors de la consultation de 2024 ont été mises en œuvre dans le cadre du budget 2025.

Secteur des télécommunications

Dans de nombreux dossiers de fraude que nous voyons à l'OSBI, les réseaux et équipements de télécommunications sont un élément important de la communication entre le criminel et la victime et, dans certains dossiers, ils donnent de la crédibilité ou une apparence d'authenticité aux stratagèmes frauduleux. Par exemple, dans de nombreux dossiers où la fraude a été initiée par téléphone, l'afficheur indique que le nom et le numéro de l'appelant correspondent à ceux d'une institution financière. Il est de notre compréhension que ces appels sont souvent effectués auprès de nombreuses victimes potentielles simultanément ou presque simultanément.

Notre expérience nous porte à croire que les exploitants de systèmes de télécommunications ont l'occasion de jouer un rôle clé de gardien dans les initiatives canadiennes de lutte contre la fraude. Par exemple, en traitant les systèmes technologiques qui permettent l'usurpation du numéro d'appelant, en mettant en place des mécanismes pour détecter les schémas d'utilisation typiquement employés par des acteurs frauduleux, et en bloquant l'accès aux réseaux de télécommunications lorsque de tels schémas frauduleux sont détectés. Des règles devraient être instaurées afin de contraindre les entreprises du secteur des télécommunications à mettre en place des changements et à procéder à des interventions technologiques pour saisir cette occasion visant à protéger les Canadiens contre la fraude.

Plateformes numériques

D'après notre expérience, les fraudes et les arnaques sont souvent initiées via des plateformes numériques. Les criminels qui souhaitent commettre une fraude contactent souvent leurs victimes via des plateformes de médias sociaux, des courriels et d'autres canaux de communication numériques.

Les plateformes numériques ont l'occasion d'exercer un rôle clé de gardien pour détecter et prévenir les fraudes dès leur apparition. P. ex., en identifiant les messages et le contenu promu qui présentent des caractéristiques typiques des fraudes et des arnaques, en surveillant les communications entre utilisateurs du système pour repérer un contenu suspect, et en refusant l'accès ou en interrompant les actions en ligne de personnes soupçonnées de fraude. Des règles devraient être mises en place pour exiger que les plateformes numériques développent et mettent en œuvre de telles technologies d'identification et de perturbation.

Une considération clé pour les décideurs politiques sera de déterminer s'il convient d'adopter une approche très prescriptive, exigeant des interventions ou des actions précises de la part des entreprises des secteurs bancaire, des télécommunications ou des plateformes numériques, ou de s'appuyer sur un système fondé sur des principes. Bien que des listes très précises d'exigences offrent l'avantage de la clarté et d'une application claire, elles sont peu susceptibles de rester actuelles ou pertinentes dans l'environnement en évolution rapide de la fraude en ligne. Les approches davantage fondées sur des principes sont plus susceptibles de demeurer pertinentes au fil du temps, mais elles sont moins certaines et davantage sujettes à l'interprétation par les acteurs de l'industrie et les organismes de réglementation.

18. Comment inciter les organisations à détecter efficacement les activités susceptibles d'être frauduleuses au sein de leurs services et à mener des enquêtes à leur sujet?

Les incitatifs sont les plus forts lorsque les attentes sont accompagnées de mécanismes de responsabilisation et de responsabilité juridique. Comme nous l'avons indiqué dans notre mémoire envoyé au ministère des Finances en septembre 2024, l'OSBI estime que transférer la responsabilité des préjudices causés par la fraude de la victime aux fournisseurs de services, dans des circonstances où il n'y a pas eu de négligence grave de la part de la victime, constituerait une incitation puissante pour tous les participants du Cadre à s'engager sérieusement à prendre des initiatives anti-fraude.

En transférant la responsabilité de la fraude aux participants du Cadre, les institutions auront une motivation financière immédiate à développer et mettre en œuvre des mécanismes de détection et de prévention pour leurs clients, et à maintenir et mettre à jour ces systèmes au fur et à mesure que l'environnement de fraude évolue au fil du temps.

Ainsi, bien que nous appuyions les propositions de détection et de prévention de la fraude énoncées dans le document de consultation, notre position générale est qu'un système basé sur la responsabilité est préférable, ou serait complémentaire à de telles exigences prescriptives.

La responsabilité des préjudices subis par des victimes de fraude n'ayant commis aucune négligence, ainsi que la répartition de la responsabilité entre les entreprises du secteur concerné par le cadre réglementaire, pourraient être soumises au respect des mesures de prévention spécifiques établies par le régulateur du cadre.

19. Comment les organisations devraient-elles être tenues d'évaluer les préjudices causés par les activités frauduleuses aux personnes qui utilisent leurs services?

Selon notre expérience, les préjudices liés à la fraude peuvent habituellement être clairement définis en termes financiers. Les fraudes sont généralement exclusivement axées sur le fait de soutirer de l'argent aux victimes, et nous évaluons habituellement que les préjudices subis correspondent au montant perdu. D'autres impacts, tels que le vol d'identité, l'atteinte au crédit, le temps et le stress importants, ainsi qu'un risque accru d'être à nouveau ciblé, sont importants et potentiellement significatifs, mais sont plus difficiles à quantifier lorsqu'il s'agit de résoudre une plainte liée à une fraude. Souvent, lorsque ces préjudices non financiers semblent importants, nous évaluerons un montant de compensation financière afin de reconnaître les impacts potentiels continus pour le consommateur. Les services continus, tels que la surveillance du crédit, peuvent également faire partie d'un ensemble de mesures de compensation.

20. Quelles mesures les organisations devraient-elles être tenues de prendre pour évaluer le risque de préjudice futur pour les personnes touchées par une activité frauduleuse?

Les organisations devraient être tenues de prendre des mesures concrètes pour réduire le risque de victimisation répétée. Cela inclut la réinitialisation des mots de passe ou des identifiants, une surveillance renforcée, des avertissements ciblés, la vérification des bénéficiaires et des coordonnées, ainsi que des directives claires pour restaurer l'identité. OBSI a vu des dossiers où des personnes ont été victimes à plusieurs reprises lorsque les vulnérabilités connues n'ont pas été prises en compte. Des attentes claires en matière de soutien de suivi-après un incident de fraude aideraient à prévenir de futures pertes et à renforcer la confiance des consommateurs.

21. Quand une organisation réglementée du secteur privé devrait-elle pouvoir communiquer des informations sur une activité frauduleuse à une autre organisation réglementée du secteur privé?

Nos points de vue sur le partage d'information entre organisations du secteur privé sont similaires à ceux décrits ci-dessus en ce qui concerne le partage d'information entre régulateurs. De façon générale, nous constatons qu'un partage accru de l'information favorise et correspond aux objectifs globaux du Cadre, sous réserve des limites entourant le partage de renseignements personnels et de la prudence quant aux conséquences potentiellement négatives d'une identification inexacte d'une personne ou d'une entité comme auteur de fraude.

Les organisations du secteur privé devraient être encouragées à partager des informations liées à la fraude lorsqu'il est nécessaire de prévenir, détecter ou perturber la fraude et de soutenir les efforts de suivi et de récupération. C'est particulièrement important pour les arnaques actives et l'identification des réseaux utilisés pour déplacer de l'argent volé.

Comme nous l'avons observé plus haut, le partage d'informations entre organisations du secteur privé pourrait permettre de perturber et de prévenir de façon significative les fraudes en cours, mais comporte aussi le risque de causer un préjudice grave à toute personne identifiée à tort. D'après notre expérience, les institutions financières ont une grande aversion au risque et sont susceptibles de refuser d'offrir des services à toute personne qu'elles considèrent comme potentiellement impliquée dans un crime ou un

acte répréhensible, ce qui peut entraîner des dommages importants pour la personne concernée. Comme mentionné ci-dessus, les personnes identifiées doivent être informées qu'elles l'ont été et avoir la possibilité de répondre et/ou de désapprouver les allégations portées contre elles.

22. Le cas échéant, quelles sont précisément les informations qui devraient être communiquées et dans quelles circonstances et à quelles fins précises devraient-elles l'être?

Le partage d'informations devrait se concentrer sur des signes et des schémas clairs susceptibles de prévenir les préjudices. Cela inclut les sites web frauduleux, les numéros de téléphone ou les adresses de portefeuille, les signes que des comptes sont utilisés pour déplacer de l'argent volé, des appareils ou des comportements, ainsi que des renseignements sur les méthodes courantes d'arnaque. L'information devrait être partagée lorsqu'elle est confirmée ou très fiable, et lorsque l'organisme récepteur peut prendre des mesures précises pour prévenir d'autres pertes ou aider à récupérer des fonds.

23. Quels mécanismes de protection de la vie privée ou de surveillance faudrait-il mettre en place pour de telles initiatives d'échange d'informations?

De fortes garanties en matière de vie privée comprennent une autorité légale claire, des limites quant à l'utilisation des renseignements, le partage uniquement de ce qui est nécessaire, un accès contrôlé, la tenue des registres d'utilisation, une surveillance indépendante, des limites sur la durée de conservation des renseignements et des moyens de corriger les erreurs. Parce que des informations incorrectes peuvent gravement nuire aux consommateurs, il est essentiel d'assurer une gouvernance solide des listes partagées, incluant des processus clairs pour réviser, mettre à jour et supprimer les informations au besoin.

24. Quand les organisations devraient-elles être autorisées à communiquer des informations sur une activité frauduleuse aux organismes d'application de la loi dans le but de prévenir, de détecter et de perturber l'activité frauduleuse et d'enquêter sur celle-ci?

25. Quand les organismes d'application de la loi devraient-ils être autorisés à communiquer des informations sur une activité frauduleuse à des organisations du secteur privé?

26. Quand le gouvernement devrait-il être autorisé à communiquer des informations sur une activité frauduleuse aux organismes d'application de la loi?

27. Quand le gouvernement devrait-il être autorisé à communiquer des informations sur une activité frauduleuse à des organisations du secteur privé?

28. Le cas échéant, quelles sont précisément les informations qui devraient être communiquées et dans quelles circonstances et à quelles fins précises devraient-elles l'être?

29. Quelles mesures de protection de la vie privée ou quels mécanismes de surveillance faudrait-il mettre en place pour de telles initiatives d'échange d'information?

Réponse aux Questions 24 à 29

Veuillez consulter notre réponse ci-dessus aux questions 8 à 11 et 21 à 23 concernant le partage d'informations entre les organismes de réglementation et les forces de l'ordre, ainsi que le partage d'informations entre les organisations du secteur privé. Nos observations générales, recommandations et mises en garde s'appliquent également au partage d'informations entre les forces de l'ordre, le gouvernement et les organisations du secteur privé.

30. Quelles règles de détection des fraudes propres aux secteurs faudrait-il mettre en place?

Tous les secteurs ont un rôle clé à jouer dans la détection et la prévention des fraudes et devraient être tenus d'assumer les fonctions de gardien appropriées à leur rôle dans les services aux consommateurs. Les règles en place pour chaque secteur devraient exiger que les acteurs de l'industrie prennent des mesures appropriées pour identifier toute activité transactionnelle inhabituelle, les signes que des comptes ont été compromis, ainsi que les tendances liées à des activités frauduleuses et au déplacement d'argent volé. Il doit également y avoir des attentes claires quant à la rapidité avec laquelle les organisations interviennent dès l'apparition de signes avant-coureurs.

Pour les plateformes numériques et les fournisseurs de services de télécommunications, utiliser des outils algorithmiques et d'intelligence artificielle pour identifier les schémas de communication liés à un risque de fraude et perturber ces communications est d'une importance cruciale. Ces plateformes sont également particulièrement placées pour fournir des avertissements en temps opportun aux utilisateurs du système lorsqu'une fraude potentielle est détectée.

Pour le secteur bancaire, comme nous l'avons observé dans notre soumission de septembre 2024, la détection de la fraude est fondamentale pour toute stratégie de prévention. Les banques canadiennes, comme les banques du monde entier, ont beaucoup investi dans des politiques et des systèmes pour détecter la fraude et les escroqueries, y compris des systèmes de vérification des clients, la surveillance des transactions en temps réel et la formation régulière des employés. Toutefois, comme nous l'avons vu, les systèmes et les processus actuellement en place n'ont pas été suffisants pour empêcher que les fraudes et les escroqueries n'aient de graves répercussions sur les consommateurs canadiens. Nous avons observé de nombreux cas où les systèmes de détection de la fraude n'ont pas réussi à protéger les consommateurs et où l'application des systèmes et des processus a été incohérente et inadéquate.

Nous avons également observé des différences importantes dans l'approche adoptée par chaque banque en matière de détection, de prévention et de correction de la fraude. En l'absence d'exigences réglementaires en matière de détection des fraudes, chaque institution détermine sa propre posture de sécurité ainsi que la priorité et l'investissement qu'elle choisit de faire au nom de ses clients. Cependant, les clients bancaires n'ont aucun moyen d'évaluer la qualité du programme de détection de fraude d'une banque et ne peuvent donc pas choisir leur banque sur cette base; il est donc impossible de se fier aux forces traditionnelles du marché pour motiver les banques à investir dans des technologies robustes de détection de fraude.

Nous croyons qu'il existe une possibilité pour les banques canadiennes d'investir dans le développement de systèmes améliorés de surveillance et de détection, y compris ceux qui analysent le comportement des consommateurs et détectent les schémas de transactions frauduleuses de manière plus précise et cohérente, et qu'il s'agit d'un domaine pertinent pour l'établissement de normes réglementaires.

Comme indiqué dans notre lettre de réponse datée de 2024, selon notre expérience, les circonstances où une détection pourrait être requise pour les acteurs du secteur bancaire comprennent :

- Les clients signalent une fraude potentielle ou expriment des préoccupations au sujet d'une ou de plusieurs transactions ou alertes
- Des tendances qui suggèrent une fraude potentielle sont détectées, telles que les circonstances suivantes, en particulier en combinaison :
    - Transactions inhabituelles qui ne correspondent pas au comportement habituel du consommateur
        - Nouveaux types de transactions pour le consommateur lorsqu'il n'a jamais utilisé le service ou le produit bancaire utilisé pour lancer la transaction
        - Un montant de transfert beaucoup plus élevé que ce qui est typique pour le consommateur
        - Fréquence et/ou nombre inhabituels de transferts
        - Transferts à un moment de la journée qui n'est pas normal pour le consommateur, par exemple entre 1 et 5 heures du matin, heure locale
        - Transferts à un destinataire dans une région géographique où le consommateur n'a pas de lien antérieur
        - Connexions à partir d'une adresse IP inhabituelle, en particulier une adresse géographiquement éloignée de l'emplacement normal du consommateur
    - Transactions qui correspondent à des modèles connus d'activités frauduleuses, telles que la réception de multiples virements électroniques suivis de virements électroniques immédiats hors du compte
    - Transferts à un ou plusieurs nouveaux bénéficiaires
    - Transactions liées à des personnes ou à des comptes précédemment impliqués dans des fraudes ou des escroqueries
    - Transferts multiples légèrement inférieurs ou à la limite quotidienne
    - Transferts à des destinataires à risque plus élevé, y compris des sites de paiement comme Wise et Western Union ou des jeux de hasard en ligne, des sites de cryptomonnaies non autorisés et des sites pour adultes, en particulier lorsque le consommateur n'a pas d'antécédents de transferts antérieurs
    - Connexions multiples à partir d'emplacements géographiquement éloignés dans un court laps de temps
    - Transferts initiés via un appareil nouvellement ajouté ou rarement utilisé
    - Transferts dans un compte avant un virement électronique, p. ex. d'une marge de crédit ou d'une carte de crédit à un compte chèques ou d'épargne immédiatement avant les virements électroniques
    - Modifications de compte inhabituelles ou tentatives de modification de compte, par exemple la modification de renseignements de base (mot de passe, numéro de téléphone,

adresse courriel, mode de réception du code à usage unique) immédiatement avant le virement électronique d'une somme importante ou de nombreux virements électroniques très rapprochés de petits montants qui, additionnés, s'élèvent à une somme importante
    - Échec des connexions ou des tentatives de changement de mot de passe peu de temps avant une demande de transfert
- Les consommateurs sont vulnérables ou présentent un risque plus élevé de fraude, par exemple dans les cas suivants :
    - Le consommateur n'a aucune présence technologique (c.-à-d. pas de profil bancaire en ligne, pas d'ordinateur, pas de courriel ni aucune autre technologie
    - Le consommateur est une personne âgée
    - Le compte est contrôlé au moyen d'une procuration
    - Le consommateur a déjà été victime de fraude
- Interactions téléphoniques inhabituelles avec les services bancaires, par exemple, lorsqu'un prétendu consommateur appelle la banque et n'arrive pas à répondre aux questions de vérification ou qu'il tente de contourner les procédures normales en prétendant ne pas avoir accès aux messages texte ou qu'il refuse la vérification à l'aide d'un code unique
- Transactions qui dépassent une limite quotidienne établie
- Augmentations de la limite quotidienne immédiatement avant les transferts
- Toute incapacité à répondre avec exactitude aux messages texte ou aux appels téléphoniques de vérification

31. Comment trouver un équilibre pour limiter l'utilisation des infrastructures des secteurs d'activité à des fins frauduleuses, tout en veillant à ce que les utilisateurs légitimes ne soient pas déraisonnablement privés de l'utilisation des services?

Bien que les mesures de détection et de prévention de la fraude soient susceptibles d'introduire des frictions et des retards pour les consommateurs de services financiers, un certain degré d'inconvénient est justifié compte tenu des conséquences potentiellement dévastatrices de la fraude.

Si tous les intervenants du secteur sont tenus aux mêmes normes de détection et de prévention, nous nous attendons à ce qu'ils investissent dans le développement de mécanismes innovants pour offrir ces protections, tout en cherchant à gagner des parts de marché et à offrir des services à un niveau acceptable pour les consommateurs. Chaque fournisseur de services mettrait probablement en place des interventions qui équilibrent ses exigences réglementaires et la protection des consommateurs avec l'attrait et l'utilisabilité de ses offres. Nous nous attendons à ce que cela implique moins de mesures de protection intrusives dans les situations à faible risque et des mesures supplémentaires dans les situations à plus haut-risque.

Pour protéger les utilisateurs légitimes, les fournisseurs de services pourraient utiliser des mécanismes tels que des notifications rapides, des explications claires de toute restriction et des possibilités simples pour les consommateurs de rétablir les services lorsque c'est approprié, avec une attention particulière pour les personnes plus vulnérables.

Il est important de noter que si les consommateurs ont choisi de désactiver l'accès à des produits et services bancaires particuliers, en particulier toute fonctionnalité pouvant transférer des fonds à partir d'un compte, la réactivation d'une telle fonctionnalité ne devrait pas être possible, sauf avec des outils de validation supplémentaires tels qu'une autorisation en personne.

32. Dans quelles situations les entités réglementées devraient-elles être tenues de suspendre les activités susceptibles d'être frauduleuses?

Les organisations devraient être tenues de suspendre les transactions chaque fois que des signes de fraude, comme ceux décrits ci-dessus en réponse à la question 30, sont détectés. Pour éviter des interruptions inutiles du service, des exceptions pourraient être permises, p. ex., des limites monétaires minimales. Les décideurs pourraient envisager d'établir un cadre où des pauses sont requises dans certaines circonstances et permises dans d'autres. Par exemple, des pauses pourraient être requises lorsqu'il y a un risque élevé d'arnaque ou d'activité frauduleuse et lorsqu'une pause est susceptible d'éviter une perte irréversible, et des pauses pourraient être permises dans des scénarios à moindre risque.

33. Quelles mesures de protection et de recours faudrait-il mettre en place pour s'assurer que l'accès des personnes n'est pas indûment suspendu ou retiré?

Les mesures de prévention de la fraude devraient être équitables, transparentes et réversibles. Lorsque des mesures de prévention sont prises, les consommateurs devraient être informés rapidement, avec une explication générale des raisons de l'intervention et des renseignements sur la façon de rétablir les services et/ou de faire remonter leurs préoccupations. Si l'accès est indûment limité, les organisations devraient le rétablir rapidement et offrir des mesures de réparation appropriées, ainsi que des options claires pour transmettre les plaintes à un niveau supérieur.

34. Comment assurer l'efficacité des notifications d'activités frauduleuses présumées?

Les notifications sont les plus efficaces lorsqu'elles sont opportunes et exploitables. L'OSBI appuie l'obligation que les notifications avertissent clairement les consommateurs de tout risque détecté et qu'elles soient transmises le plus tôt possible, de préférence lorsque le consommateur est encore en mesure de stopper ou de modifier la transaction. L'utilisation de plusieurs canaux de communication est essentielle, particulièrement lorsqu'un canal peut être compromis par l'acteur frauduleux. Les notifications devraient être exprimées dans un langage clair et simple et indiquer clairement les prochaines étapes que le consommateur peut suivre pour régler le problème, par exemple : « répondez STOP pour geler ce compte ».

35. Quelles règles sectorielles de perturbation de la fraude faudrait-il mettre en place?

De même que dans notre réponse à la question 32 ci-dessus concernant la suspension des transactions, les organisations devraient être tenues de perturber les transactions dès que des signes de fraude, tels que ceux décrits ci-dessus en réponse à la question 30, sont détectés. Pour éviter des interruptions inutiles du service, des exceptions pourraient être permises, p. ex., des limites monétaires minimales.

Les décideurs pourraient également envisager d'établir un cadre dans lequel la perturbation serait requise dans certaines circonstances et permise dans d'autres. Par exemple, une perturbation pourrait être requise pour des transactions de grande valeur ou lorsqu'il existe un haut degré de certitude qu'une arnaque ou une activité frauduleuse est en cours et que la perturbation est susceptible d'empêcher une perte irréversible, tandis qu'elle pourrait être permise dans des scénarios de moindre valeur et/ou de moindre certitude.

Règles claires, spécifiques à chaque secteur-qui établissent des attentes de base quant à la manière dont les organisations devraient perturber la fraude dans des situations à risque élevé-devraient être en place. Cela pourrait inclure des règles stipulant :

- Pauses de communication ou de transaction requises ou attendues lorsqu'on détecte des signes d'alerte
- mesures immédiates pour geler, récupérer ou tracer les fonds
- Exigences de coopération entre organisations au sein et entre les secteurs pour contrer les fraudes actives

Il convient également de tenir compte des conséquences imposées aux organisations en cas de non-intervention contre les fraudes et arnaques conformément aux règles. Imposer une responsabilité financière pour de tels échecs aidera à s'assurer que les organisations investissent dans la capacité d'agir rapidement et de manière constante.

Les consommateurs devraient aussi être dotés d'outils qu'ils peuvent utiliser pour perturber les fraudes ou les arnaques s'ils soupçonnent que leur compte a pu être compromis, ou en réponse aux avertissements qu'ils ont reçus. De tels outils devraient inclure la capacité de geler des comptes ou certaines fonctionnalités du compte, p. ex., la possibilité de geler tous les transferts hors du compte.

36. De quelle manière les organisations devraient-elles être tenues de faciliter la tâche des utilisateurs lorsqu'ils doivent signaler une activité frauduleuse?

Les organisations devraient offrir des moyens faciles et accessibles pour que les consommateurs signalent la fraude, par exemple au moyen d'une application, d'un site web ou par téléphone. Les consommateurs devraient avoir la possibilité de verrouiller immédiatement leurs comptes ou certaines fonctionnalités de leur compte et devraient être invités à fournir toute preuve susceptible d'être pertinente à la détection ou à la prévention de fraudes similaires dans d'autres comptes. Les consommateurs qui signalent des soupçons de fraude devraient recevoir une confirmation rapide que leur signalement a été reçu. Ils devraient aussi recevoir une explication claire de ce qui va se passer ensuite et combien de temps cela pourrait prendre, avec un soutien supplémentaire pour les personnes vulnérables. D'après notre expérience, des processus de réception inefficaces, de longs délais d'attente, des lacunes dans la formation du personnel et des procédures d'authentification des clients difficiles ou longues peuvent grandement nuire à l'interruption rapide des activités frauduleuses, à l'enquête et à la résolution.

37. Comment les organisations pourraient-elles enquêter efficacement sur les plaintes intersectorielles?

Enquêter efficacement sur des plaintes impliquant plusieurs entreprises, en particulier des entreprises de secteurs différents, est probablement très difficile. D'après notre expérience, les plaintes impliquant plusieurs entreprises sont généralement examinées de manière isolée par chaque entreprise concernée. Parfois, cela suffit et l'entreprise responsable de l'erreur reconnaît sa responsabilité et traite la plainte de manière appropriée. Souvent, cependant, lorsque la responsabilité est partagée ou incertaine, aucune des entreprises n'accepte la responsabilité ou subordonne son acceptation à celle de l'autre entreprise.

Idéalement, les organisations impliquées dans le même incident frauduleux travailleraient ensemble pour partager l'information et la responsabilité, lorsque c'est approprié. En pratique, toutefois, lorsque plusieurs entreprises ou secteurs sont impliqués, des investigations fragmentées et la poursuite d'intérêts propres risquent de réduire considérablement la rapidité de l'enquête et la résolution équitable de la plainte, laissant les consommateurs aux prises avec plusieurs démarches de plaintes non productives simultanément. Pour éviter ce résultat, il pourrait falloir l'intervention d'un tiers indépendant, qui pourrait agir comme coordonnateur central de la plainte et faciliter des résolutions équitables et partagées lorsque cela est approprié. Par exemple, le tiers indépendant pourrait accomplir les fonctions suivantes :

- Recevoir la plainte du consommateur et clarifier les allégations contre tous les participants de l'industrie concernés
- Communiquer la plainte à tous les acteurs de l'industrie
- recevoir les résultats de l'enquête de tous les participants de l'industrie, en travaillant avec eux pour clarifier toute incohérence
- Déterminer une répartition équitable de la responsabilité si plusieurs participants de l'industrie partagent la faute
- Coordonner la communication des conclusions de l'enquête et des recommandations de règlement avec le consommateur.

38. De combien de temps les organisations devraient-elles disposer pour enquêter à l'interne sur les plaintes?

Aujourd'hui, les banques réglementées au niveau fédéral ont jusqu'à 56 jours pour enquêter et résoudre les plaintes en interne avant que les consommateurs puissent soumettre leur dossier à l'OSBI. Ce délai s'est avéré viable en pratique et donne aux consommateurs un droit clair de porter leur plainte à un niveau supérieur lorsque les processus internes ne sont pas finalisés en temps opportun ou sont autrement insatisfaisants.

Étant donné que de nombreuses plaintes relevant du Cadre concernent probablement des banques, il serait pertinent d'harmoniser les délais d'enquête du Cadre avec ceux prévus par la Loi sur les banques. Disposer d'un délai d'enquête harmonisé pour l'ensemble des organisations réglementées serait cohérent, facile à communiquer et pertinent dans ce contexte.

39. Quels renseignements les organisations devraient-elles être tenues d'inclure dans un résumé de plainte?

Les résumés de clôture des plaintes doivent fournir des renseignements clairs, complets et normalisés permettant au consommateur, à l'organisation, aux autorités de réglementation et à tout organisme externe de traitement des plaintes de comprendre la nature du différend, les éléments examinés et les motifs de toute résolution proposée. Le résumé devrait également fournir aux consommateurs des renseignements sur les prochaines étapes qu'ils peuvent suivre pour porter leur plainte à un niveau supérieur s'ils ne sont pas satisfaits.

Le contenu des lettres de réponse motivée des institutions financières adressées aux plaignants est prescrit par la réglementation dans les secteurs des valeurs mobilières et des services bancaires. Il existe un consensus raisonnable quant aux meilleures pratiques pour ces lettres.

Par exemple, la règle 3756 de l'organisme canadien de réglementation des investissements (OCRI), qui a été récemment mise à jour et se trouve actuellement à l'étape finale de son processus de consultation publique, propose les exigences suivantes :

- Des lettres de réponse substantielles doivent être envoyées à chaque plaignant.
- La lettre de réponse substantielle doit être rédigée en langage clair et dans un format facilement accessible et compréhensible pour le plaignant.
- La lettre de réponse substantielle doit inclure les informations suivantes :
    - Un résumé de la plainte,
    - le résultat de l'enquête de l'entreprise,
    - la décision de l'entreprise concernant la plainte, y compris une explication des facteurs ayant mené à cette décision,
    - une déclaration expliquant au consommateur les options disponibles si celui-ci n'est pas satisfait de la réponse de l'entreprise, y compris la disponibilité du service d'ombudsman agréé et les éventuelles restrictions temporelles pour les démarches d'escalade qui pourraient s'appliquer
    - Déclaration selon laquelle le consommateur peut présenter une plainte au régulateur afin qu'il puisse évaluer s'il convient de prendre une mesure disciplinaire.

De même, l'Agence de la consommation en matière financière du Canada précise le contenu prescrit des lettres de réponse substantielle dans sa publication *Ligne directrice sur les procédures de traitement des plaintes* (publiée en 2022 et actuellement en cours d'examen). La ligne directrice comprend les exigences suivantes à l'article 48 :

- La réponse écrite substantielle doit fournir toutes les informations dont un consommateur a besoin pour prendre une décision éclairée quant à la soumission ou non de la plainte à l'organisme externe des plaintes de la Banque, s'il le souhaite, y compris :
    - La date à laquelle la plainte a été communiquée à la banque
    - le fait que la période prescrite est écoulée et que la banque n'a pas pu résoudre la plainte dans ce délai, le cas échéant

- Une déclaration des faits relatifs à la plainte
- La décision finale de la Banque et, le cas échéant, son offre en réponse à la plainte, ainsi que toute information pertinente sur le processus ayant mené à cette décision finale.
- la méthode utilisée pour calculer l'indemnisation (monétaire ou non monétaire), le cas échéant
- le droit du consommateur de présenter sa plainte à l'organisme externe chargé des plaintes ainsi que la manière de le contacter

L'OSBI a publié des lignes directrices à l'intention des entreprises, intitulées *Établir et communiquer votre processus de gestion des réclamations*, qui précisent que les lettres de réponse finale des entreprises devraient inclure :

- Description de la plainte
- Les résultats de l'enquête de la firme
- Une justification de la décision
- Un dernier paragraphe précisant la possibilité de recourir à l'OSBI, formulé ainsi : « Si vous n'êtes pas satisfait de notre réponse, vous pouvez transmettre votre plainte à l'Ombudsman des services bancaires et d'investissement (OSBI). » OSBI est un service indépendant de résolution des différends qui enquête sur les différends non résolus sans frais pour vous. Une alternative au système juridique, il peut recommander une indemnisation allant jusqu'à 350 000 $. Vous pouvez joindre l'OSBI au 1-888-451-4519 ou à www.obsi.ca, et vous devez le contacter dans les 180 jours suivant la réception de cette réponse finale à votre plainte.

40. Les organisations devraient-elles être tenues responsables lorsqu'elles ne respectent pas leurs obligations prévues dans le cadre?

Comme nous l'avons indiqué dans notre réponse à la question 18 se rapportant à notre soumission au ministère des Finances en septembre 2024, l'OSBI croit que le fait de transférer la responsabilité des préjudices causés par la fraude de la victime aux fournisseurs de services, sauf en cas de négligence grave de la part de la victime, constituerait une incitation puissante pour tous les participants du Cadre à s'engager sérieusement à prendre des initiatives de lutte contre la fraude.

En transférant la responsabilité de la fraude aux participants du Cadre, les institutions auront une motivation financière immédiate à développer et mettre en œuvre des mécanismes de détection et de prévention pour leurs clients, et à maintenir et mettre à jour ces systèmes au fur et à mesure que l'environnement de fraude évolue au fil du temps.

La responsabilité des préjudices subis par des victimes de fraude n'ayant commis aucune négligence, ainsi que la répartition de la responsabilité entre les entreprises du secteur concerné par le cadre réglementaire, pourraient être soumises au respect des mesures de prévention spécifiques établies par le régulateur du cadre.

41. Quelles normes devraient s'appliquer pour déterminer si une organisation a rempli ou non ses obligations?

Pour établir des normes et évaluer si une organisation a rempli ses obligations, les facteurs suivants sont particulièrement pertinents :

- Si des contrôles appropriés étaient en place et fonctionnaient efficacement, y compris des mesures d'authentification, la surveillance des transactions et des outils de détection de fraude proportionnellement au profil de risque de l'activité.

- Si l'organisation a réagi rapidement une fois les indicateurs de risque déclenchés, notamment en appliquant des mesures de protection telles que des avertissements, une vérification renforcée, des blocages temporaires ou des suspensions, des rappels ou des annulations de transactions lorsque cela est possible.

- Si des mesures ont été prises en temps opportun pour prévenir ou limiter les préjudices, reconnaissant que les retards peuvent réduire considérablement la probabilité de récupérer les fonds dans les dossiers de fraude.

- À savoir si les communications avec le consommateur étaient opportunes, claires et exploitables, y compris les avertissements, les explications des risques et les conseils sur les prochaines étapes.

- Si les processus de traitement des plaintes et d'enquête respectaient les normes de service applicables, y compris la coopération avec d'autres parties lorsque requis et la conservation des preuves pertinentes.

42. Comment la responsabilité devrait-elle être répartie lorsque plusieurs organisations n'ont pas rempli leurs obligations?

La responsabilité devrait être répartie selon le degré de contrôle de chaque organisation sur le point de risque pertinent et sa contribution à la défaillance (p. ex., lacunes en matière d'identité/authentification, défaillances de surveillance, manque d'action sur les indicateurs, retards dans les mesures de récupération ou manque de coopération). Pour protéger les consommateurs, les décideurs devraient éviter les modèles qui laissent les particuliers sans indemnisation tant que les institutions débattent de la responsabilité. Une approche axée sur le consommateur — où l'indemnisation a lieu rapidement et où la répartition des responsabilités est réglée entre les organisations par la suite — peut diminuer les délais et renforcer l'équité.

D'un point de vue pratique, la répartition de la responsabilité entre les fournisseurs de services risque d'être controversée et difficile à résoudre sans directives claires et/ou supervision externe. Une telle répartition pourrait reposer sur une présomption de responsabilité partagée à parts égales, avec une obligation pour les fournisseurs de services qui estiment avoir moins de responsabilités de démontrer qu'une autre répartition serait plus juste. Le régulateur du cadre pourrait assumer la supervision des

différends de répartition non résolus, ou cette responsabilité pourrait être déléguée à l'organisme externe de traitement des plaintes.

43. Quels sont les critères qui devraient guider le choix d'un organe externe chargé de traiter les plaintes?

À titre préliminaire, il convient de donner la priorité à l'assurance que les consommateurs aient accès à un service d'ombudsman indépendant et accessible pour les plaintes non résolues découlant du cadre proposé.

Comme il est indiqué dans notre octobre 2021 soumission à la consultation du ministère des Finances sur le renforcement du système externe de traitement des plaintes du Canada, l'accès à un service d'ombudsman équitable, efficace et de confiance est reconnu internationalement comme un élément essentiel du cadre de protection des consommateurs financiers d'un pays, car :

- Elle offre un accès à la justice aux consommateurs qui se retrouvent en litige avec leur fournisseur de services financiers.
- Elle répond aux attentes des consommateurs en matière de traitement équitable et soutient la confiance des consommateurs dans le secteur des services financiers.
- Elle encourage une gestion efficace des plaintes au niveau de l'entreprise.
- Elle fournit de l'information aux régulateurs, aux acteurs de l'industrie et au public sur les expériences difficiles des consommateurs, alimentant ainsi un cercle vertueux d'amélioration systémique.

De plus, la structure de l'OETP pour le cadre proposé qui répondrait le mieux aux besoins des Canadiens serait un service d'ombudsman financier unique, mandaté et responsable auprès du régulateur du cadre. Dans notre soumission de 2021, nous avons également décrit en détail les raisons pour lesquelles la concurrence entre l'OETP n'est pas dans l'intérêt public et soulève une crainte raisonnable de partialité. Il y a cinq principaux problèmes liés à la concurrence entre organismes externes de traitement des plaintes (OETP) :

- Confusion des consommateurs
- Biais systémique réel et perçu à l'égard des fournisseurs de services financiers qui choisissent l'ombudsman
- Lacunes pour les dossiers impliquant plusieurs institutions
- Diminution de la valeur informationnelle des données désagrégées
- Réduction de l'efficacité liée aux économies d'échelle et à l'étendue

Le choix d'un organisme externe de traitement des plaintes relevant du Cadre devrait être fondé principalement sur le fait que cet organisme dispose de la structure, de l'expérience et des capacités nécessaires pour résoudre un volume élevé de plaintes impliquant des préjudices financiers potentiellement importants. En particulier, il faut examiner si l'organisme :

- Est constitué spécifiquement pour résoudre les différends des consommateurs du secteur financier, notamment les plaintes portant sur la responsabilité contestée, les pertes financières et l'indemnisation.

- Possède une expérience dans un cadre législatif et réglementaire clair, avec des obligations de reddition de comptes définies, incluant des exigences de rapport, des normes de service et des mécanismes d'examen indépendants.

- Fait preuve d'indépendance et d'impartialité, soutenues par des mécanismes de gouvernance qui protègent la prise de décision contre l'influence des entreprises participantes et garantissent des processus et des résultats équitables.

- Expertise et capacité d'enquête pour évaluer les plaintes concernant des produits financiers complexes, des contrôles internes, des processus d'authentification et des obligations de protection des consommateurs, y compris lorsque des problèmes tels que la fraude ou des transactions non autorisées sont allégués.

- Fournit des processus accessibles, transparents et cohérents, sans frais pour les consommateurs, incluant une assistance tout au long du processus de plainte et une communication claire des conclusions et résultats dans les deux langues officielles.

- Produit des résultats opportuns et raisonnés, incluant des recommandations d'indemnisation lorsque cela est approprié, appuyées par des méthodologies établies et des indicateurs de performance rendus publics.

- Est en position d'identifier et d'escalader les problèmes systémiques, afin que les tendances des plaintes puissent éclairer le travail de supervision et de politique des régulateurs.

44. Les décisions de l'organe externe chargé de traiter les plaintes devraient-elles être exécutoires?

À notre avis, donner à l'OETB le pouvoir de rendre des décisions contraignantes dans le cadre proposé serait idéal, mais ce n'est pas nécessaire pour profiter de bon nombre des avantages du système OETB.

Au cours des trente années où OSBI a travaillé avec les banques et leurs clients pour résoudre des différends, les banques ont presque toujours proposé de régler les différends des consommateurs conformément à nos recommandations. Cela contraste avec notre expérience avec les firmes de valeurs mobilières. En ce qui concerne notre mandat en matière de valeurs mobilières, l'OBSI revendique depuis longtemps des pouvoirs accrus pour assurer une réparation, principalement parce que le système actuel de « dénonciation publique » permet aux firmes d'agir selon l'incitatif économique qu'elles ont à proposer de régler les plaintes à des montants inférieurs (parfois bien inférieurs) à ceux que nous considérons comme équitables dans toutes les circonstances du dossier, et ne donne aux consommateurs aucune autre option réaliste que d'accepter de tels règlements. La pratique de dénoncer et de blâmer, lorsqu'elle se produit, contribue également à ternir injustement l'image de l'industrie dans son ensemble auprès du public. Ce défi a été observé de façon constante au fil du temps et a été signalé par des évaluateurs

indépendants, des défenseurs des consommateurs et des organismes de réglementation des valeurs mobilières.

Bien que nous n'ayons pas rencontré de défis similaires avec les banques — et que nous estimions généralement que le système actuel de dénonciation publique est efficace pour nous permettre de parvenir à des résolutions équitables dans les différends entre les banques et leurs clients — nous sommes conscients de la perception du public selon laquelle notre mandat non contraignant est perçu comme moins effectif ou plus faible qu'un mandat contraignant. Il n'est pas rare que notre mandat non contraignant soit qualifié de « dépourvu de mordant ».

En raison de l'importance de cette question du point de vue de la perception du public, nous recommanderions un mandat contraignant pour les différends relevant du cadre, bien que, selon nous, l'ECB serait probablement également en mesure d'assurer un règlement équitable des différends en vertu du cadre proposé avec des pouvoirs non contraignants.

45. De combien de temps l'organe externe chargé de traiter les plaintes devrait-il disposer pour enquêter sur les plaintes transmises à un échelon supérieur?

Nous croyons que toutes les parties prenantes bénéficient d'un processus de résolution des différends qui permet d'aboutir à des conclusions équitables aussi efficacement que possible. Le temps qu'un dossier nécessite pour être réglé dépend de nombreux facteurs, notamment la nature de la plainte, les preuves disponibles, la complexité du dossier et la disponibilité ou la participation de l'entreprise et du consommateur.

En vertu de la Loi sur les banques, l'OSBI est tenu de résoudre toutes les plaintes en matière de services bancaires — y compris celles liées à la fraude — dans un délai maximal de 120 jours. Selon l'expérience de l'OSBI dans l'examen des plaintes, la plupart des dossiers bancaires sont réglés en moins de 60 jours, presque tous le sont en moins de 90 jours, et certains dossiers très complexes nécessitent jusqu'à 120 jours.

Nous estimons qu'il serait judicieux que les délais de résolution des plaintes dans le cadre réglementaire soient harmonisés avec ceux établis par la Loi sur les banques. Cela garantirait que l'OETP dispose de suffisamment de temps pour mener à bien son travail et permettrait une communication claire des échéances aux parties prenantes concernées.

46. Comment le gouvernement peut-il sensibiliser davantage les Canadiens à la menace que représente la fraude et mieux les aider à se protéger contre la fraude?

Le public canadien bénéficie des efforts de sensibilisation à la fraude déployés par de nombreuses parties prenantes clés, y compris le gouvernement du Canada. L'ACFC en particulier a accompli un travail excellent et considérable dans ce domaine, tout comme le Centre antifraude du Canada, les organismes de réglementation des valeurs mobilières canadiennes, les journalistes des médias traditionnels et d'autres. Ce message public a sans aucun doute accru la sensibilisation des Canadiens à la fraude en général, mais n'a clairement pas suffi à donner pleinement aux Canadiens les moyens de se protéger.

La technologie moderne offre des possibilités inédites pour l'éducation du public dans ce domaine, en facilitant la transmission d'informations et de messages hautement ciblés à des étapes cruciales du processus décisionnel des consommateurs. Les institutions financières, les entreprises de télécommunications et les plateformes numériques occupent une position privilégiée pour fournir des avertissements et des messages importants et ciblés aux consommateurs lors de moments déterminants dans leur processus décisionnel.

47. Comment le gouvernement peut-il sensibiliser davantage les Canadiens au risque d'utilisation à mauvais escient des identifiants émis par le gouvernement, y compris les numéros d'assurance sociale?

Le gouvernement peut accroître la sensibilisation par l'entremise de directives simples sur les situations où des identifiants comme les NAS sont légitimement requis, comment les fraudeurs les détournent, et quelles mesures immédiates doivent être prises par les consommateurs en cas de compromission soupçonnée. De plus, limiter la collecte inutile d'identifiants et promouvoir des outils pratiques de récupération (p. ex., les alertes de crédit et les voies de signalement) peut réduire les préjudices. Toute approche devrait être accessible et adaptée à différents niveaux de littératie numérique des consommateurs.

48. Qu'est-ce qui peut être fait pour soutenir la capacité des organismes d'application de la loi fédéraux à enquêter sur les actes frauduleux et à recueillir du renseignement sur la fraude?

Nous n'avons aucun commentaire en réponse à cette question.

49. Que faudrait-il faire pour améliorer la coordination entre les organismes d'application de la loi canadiens à l'échelle fédérale, provinciale, territoriale et municipale, ainsi qu'entre ces organismes et leurs partenaires internationaux?

Nous n'avons aucun commentaire en réponse à cette question.

50. Quel rôle le CAFC devrait-il jouer dans l'avancement de la stratégie?

Nous n'avons aucun commentaire en réponse à cette question.

En terminant, nous vous remercions de nous donner l'occasion de participer à cette importante consultation. Nous serions heureux de fournir d'autres commentaires au ministère des Finances en tout temps.

Cordialement,

Sarah P. Bradley
Ombudsman et chef de la direction