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

11 septembre 2024

Envoyé par courriel à : legreview-examenleg@fin.gc.ca

Directeur général
Division des institutions financières
Direction de la politique du secteur financier
Ministère des Finances Canada
90, rue Elgin
Ottawa (Ontario) K1A 0G5

Objet : Réponse à la demande de commentaires sur les propositions visant à renforcer le secteur financier du Canada

C'est avec plaisir que l'Ombudsman des services bancaires et d'investissement (OSBI) transmet ses commentaires au ministère des Finances Canada en réponse à la consultation que ce dernier a récemment menée *sur les propositions en vue de renforcer le secteur financier canadien* (le « document de consultation »).

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 27 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.

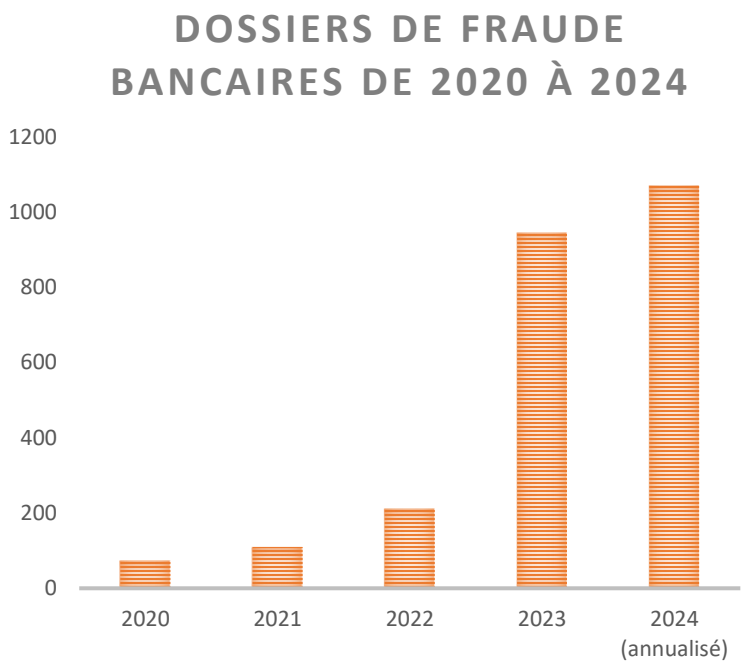
En tant que défenseurs de longue date d'un secteur des services financiers équitable, efficace et fiable, nous appuyons l'objectif global de cette consultation, en particulier l'accent mis en temps opportun sur la protection des consommateurs et la façon de mieux protéger les consommateurs et les entreprises du Canada contre la fraude. L'amélioration des systèmes de détection et de prévention de la fraude est une importante initiative de protection des consommateurs qui renforcera la confiance des consommateurs dans le système bancaire canadien ainsi que l'équité, la stabilité et la prospérité du secteur canadien des services financiers dans son ensemble.

L'expérience de l'OSBI en matière de fraude bancaire

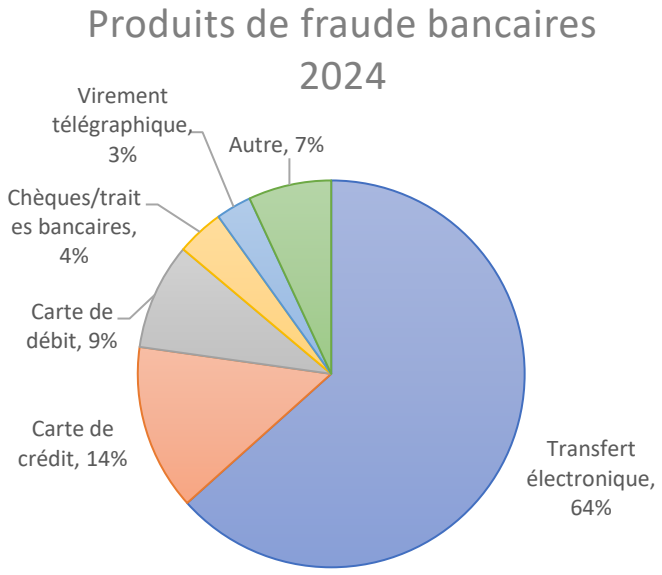
Les cas de fraude, en particulier la fraude par transfert électronique et d'autres types de fraude numérique, ont eu des répercussions sur un nombre sans précédent de consommateurs canadiens au cours de la période qui a suivi la pandémie. Cette situation s'est traduite par l'augmentation spectaculaire du nombre de plaintes portant sur ces questions que les consommateurs ont transmises à l'OSBI au cours des dernières années.

En 2021, l'OSBI a ouvert 110 dossiers liés à la fraude bancaire. En 2022, ce nombre avait presque doublé pour atteindre 213 cas. En 2023, nous avons ouvert 946 dossiers liés à la fraude, soit une augmentation de 350 % d'une année à l'autre, et cette année, nous sommes en voie d'ouvrir environ 1160 dossiers. Parmi les cas de fraude bancaire que nous avons ouverts en 2024, 68 % concernent les virements électroniques (y compris les transferts d'argent mondiaux), 12 % aux cartes de crédit et 8 % aux cartes de débit.

Une partie de cette augmentation du volume de plaintes est associée à d'importants changements apportés 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. Toutefois, nous constatons que cette augmentation de la fraude bancaire au Canada reflète également un phénomène mondial plus vaste. Les services d'ombudsman financier du monde entier signalent des augmentations tout aussi importantes des cas de fraude bancaire.



Dans bon nombre de ces cas, le consommateur admet, ou les dossiers de la banque indiquent, que le consommateur a partagé sans le savoir ses renseignements bancaires confidentiels (numéro de carte, codes d'accès et/ou numéro d'authentification à deux facteurs) avec un criminel. Les consommateurs partagent cette information soit en se faisant duper (p. ex. par un criminel se faisant passer pour un employé de banque), soit en donnant par inadvertance à un criminel l'accès à leur appareil (p. ex. en cliquant sur le lien d'un criminel qui semblait légitime).



En 2023, environ un cas de fraude sur cinq a donné lieu à un règlement ou à une recommandation d'indemnisation du consommateur. Dans la plupart des cas, nous ne sommes pas en mesure de recommander une indemnisation parce que nous n'avons aucune base légale ou réglementaire pour le faire. Le partage de renseignements bancaires confidentiels, intentionnellement ou non, constitue une violation de l'entente conclue par les consommateurs lors de l'ouverture d'un compte bancaire, ce qui les rend responsables de leurs pertes dans la plupart des cas de fraude. Les banques ont une obligation restreinte de protéger leurs clients contre ces crimes.

Lorsque nous recommandons une indemnisation dans des dossiers de fraude, c'est généralement parce que nous avons déterminé que la banque n'a pas respecté les obligations qui lui incombaient au titre du *Code de pratique canadien des services de cartes de débit* (le Code des cartes de débit) ou du *Code de conduite pour la prestation de services bancaires aux aînés* (le Code des aînés), qu'elle n'a pas été à la hauteur de ses représentations publiques sur la détection et la prévention de la fraude ou qu'elle n'a pas réussi à prévenir une fraude alors qu'elle avait manifestement l'occasion de le faire.

Nous remarquons que pour les virements électroniques, il n'y a actuellement aucune loi ou réglementation spécifique en place décrivant les obligations des consommateurs ou des banques. Par conséquent, les obligations entre les deux parties se fondent sur la convention de compte de la banque. Chaque banque possède sa propre convention qui prévoit des responsabilités différentes, y compris les attentes de la banque quant à la protection, par les consommateurs, de leurs renseignements, et aucune limite de responsabilité appliquée. Lorsque les banques offrent une restitution, elles le font souvent comme un geste de bonne volonté.

D'après notre expérience, les consommateurs croient souvent à tort qu'ils sont protégés contre la fraude et que leur banque retournera tout l'argent qu'ils ont perdu à la fraude. Cette attente des consommateurs est probablement fondée sur la compréhension générale et la publicité des protections de « responsabilité zéro » pour les produits de cartes de crédit, les représentations publiques des banques au sujet de la sécurité et de la protection contre la fraude, et la réputation générale des banques en tant que lieux sûrs et sécurisés pour la conservation des dépôts des consommateurs.

Exemple 1 - Un cas courant de fraude par virement électronique

M. E. détenait des comptes chèques et des comptes d'épargne personnels à sa banque. Il a trouvé les services bancaires en ligne sur son ordinateur portable et son téléphone cellulaire pratiques et a fréquemment accédé à ses comptes via l'application mobile de sa banque. Sa banque lui a envoyé des notifications par courriel sur l'activité de son compte, et il a souvent confirmé les soldes de son compte en ligne. Il protégeait ses appareils avec des mots de passe et les gardait confidentiels.

Un jour, M. E a reçu un avis de sa banque indiquant que le solde de son compte chèques était faible. Il s'est connecté à son compte pour enquêter et n'a rien trouvé d'inhabituel. Peu de temps après, cependant, il a reçu une autre notification confirmant deux virements électroniques de son compte. Il n'a pas reconnu les transactions, alors il s'est de nouveau connecté à son compte au moyen des services bancaires en ligne et a découvert que deux virements électroniques de 3 000 $ chacun avaient été effectués à partir de son compte.

Étant donné que l'argent n'est généralement pas recouvrable une fois transféré aux criminels, la prévention des transferts frauduleux, grâce à l'éducation des consommateurs, à l'amélioration des mécanismes de détection, à l'amélioration de la conception des produits bancaires, à l'amélioration de l'application de la loi et à la coopération entre les fournisseurs de services dont l'infrastructure est utilisée pour faciliter la fraude bancaire, est essentielle pour réduire les préjudices causés par ces crimes et préserver la confiance du grand public dans les banques canadiennes.

Le coût de la protection des consommateurs

Nous notons que toutes les propositions incluses dans le document de consultation auront des répercussions financières importantes pour les institutions financières sous réglementation fédérale du Canada. Les mécanismes améliorés de détection et de prévention de la fraude sont des entreprises coûteuses et complexes pour toute institution et tout régime de responsabilité aura également un coût financier important pour les institutions qui sont tenues d'indemniser leurs clients pour les transactions non autorisées.

Il importe toutefois de tenir compte du fait que ces coûts seront ultimement répercutés, sous forme de frais et de charges divers, sur les consommateurs pour qui les protections sont mises en œuvre. Certaines mesures imposeront des coûts indirects en causant des retards de transaction et d'autres inconvénients et frictions. De cette manière, le coût de toute mesure de protection des consommateurs prévue par la loi sera réparti entre tous les consommateurs, et la tâche des décideurs est de déterminer le niveau approprié de protection et le coût qui est justifié par les préjudices qu'ils cherchent à prévenir.

Questions de la consultation

Nos commentaires ci-dessous répondent directement aux questions précises du document de consultation. Le document de consultation émet certes des propositions importantes et potentiellement déterminantes. Cependant, dans notre soumission, nous nous concentrons principalement sur les questions posées sous le thème 2*Renforcer les mesures de protection des consommatrices et des consommateurs* et sous le thème 5 *Maintenir une réglementation de calibre mondial*, car ce sont celles qui correspondent le plus étroitement avec les domaines d'expertise de l'OSBI.

À titre préliminaire, nous notons que les questions du thème 2 comprennent trois initiatives stratégiques potentielles très interreliées :

- 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

Nous aborderons ci-dessous chacune des questions du document de consultation, séparément, dans l'ordre dans lequel elles sont posées. Cependant, à titre préliminaire, nous constatons que l'effet d'une obligation de retarder ou d'empêcher les transactions potentiellement frauduleuses dépend entièrement de la qualité des systèmes de détection de fraude dont dispose une banque. En effet, une banque ne peut empêcher une transaction que si celle-ci a été détectée avec précision. De même, un système de détection de la fraude ne peut réduire l'incidence de la fraude que s'il est utilisé pour retarder ou prévenir les transactions frauduleuses. La détection et la prévention sont les deux faces d'une même médaille, et les deux sont des exigences d'un système fonctionnel, il est donc quelque peu difficile de considérer chacun isolément.

Un régime de responsabilité limitée pourrait être mis en œuvre à la place d'exigences particulières en matière de détection et de prévention de la fraude (et non en combinaison avec de telles exigences). Si la responsabilité de la fraude est transférée aux institutions financières, ces dernières auront une incitation financière instantanée d'élaborer et de mettre en œuvre des mécanismes de détection et de prévention pour leurs clients, et de maintenir et de mettre à jour ces systèmes à mesure de l'évolution des fraudes au fil du temps.

Par conséquent, bien que dans nos commentaires ci-dessous, nous exprimions notre appui aux propositions d'exigences en matière de détection et de prévention de la fraude énoncées dans le document de consultation, cet appui est assujetti à notre opinion générale selon laquelle un système fondé sur la responsabilité est préférable à de telles exigences normatives.

Obligation de retarder ou d'empêcher les transactions

QUESTION 1 : LES BANQUES DEVRAIENT-ELLES ÊTRE TENUES D'EMPÊCHER OU DE RETARDER LES OPÉRATIONS QU'ELLES CROIENT FRAUDULEUSES OU ASSOCIÉES À UNE ESCROQUERIE, ET DANS QUELLES CIRCONSTANCES ELLES DEVRAIENT-ELLES ÊTRE TENUES D'EXERCER CETTE FONCTION?

OSBI appuie l'obligation pour les banques de retarder les transactions qu'elles croient être frauduleuses ou associées à une escroquerie. Comme il a été mentionné ci-dessus, la mise en œuvre significative de l'exigence de retarder ou d'empêcher les transactions repose entièrement sur l'exactitude et la fiabilité des mécanismes de détection d'une banque, ainsi que sur les systèmes de la banque pour intervenir rapidement lorsque de telles fraudes potentielles ont été identifiées.

Les banques ont actuellement mis en place des systèmes automatisés pour réduire et prévenir la fraude pour leurs clients, et cela est clairement important pour elles du point de vue de l'expérience client. Cependant, nous croyons qu'il existe de plus grandes possibilités de prévention de la fraude que celles que les banques utilisent actuellement. Par exemple, dans de nombreux cas, nous avons observé que les dossiers bancaires montrent une tendance anormale de comportement avant ou pendant une transaction frauduleuse qui aurait pu être détectée, comme des connexions à partir d'un emplacement géographique inhabituel, ou un transfert d'argent mondial important par une personne qui n'en a jamais envoyé auparavant, ou plusieurs transactions importantes à un nouveau bénéficiaire dans un bref laps de temps.

Exemple 2 – Le système de détection ne parvient pas à prévenir les transactions frauduleuses

Mme F détenait un compte chèques et une marge de crédit auprès de sa banque. Un jour, elle a reçu un appel téléphonique d'une personne se faisant passer pour un représentant de sa banque qui lui demandait de fournir ses renseignements bancaires ainsi qu'un code de vérification unique. Mme F a fourni les renseignements demandés à l'appelant. Par la suite, Mme F a découvert que deux virements électroniques ainsi que de nombreuses transactions avaient été effectués à partir d'un nouveau compte. Le tout s'élevait à plus de 7 400 $.

Mme F a communiqué avec sa banque pour contester les frais, mais le représentant lui a dit qu'elle en était responsable parce qu'elle avait divulgué ses renseignements bancaires à un tiers. Notre enquête a montré que les transactions effectuées ont eu lieu à peu près au même moment que plusieurs transactions refusées, ce qui avait alerté le service de la fraude de la banque d'un problème potentiel. Toutefois, mme F. n'en a jamais été informée par sa banque.

Dans certains cas, nous pouvons voir que les systèmes de détection de la fraude de la banque ont signalé les transactions comme suspectes, mais la seule mesure prise par la banque est d'envoyer un mot de passe à usage unique au consommateur. Ce type d'authentification ne protégera pas un consommateur qui a perdu le contrôle de son appareil ou qui a été trompé par un fraudeur.

Lorsque nous constatons manifestement des tendances frauduleuses sur lesquelles une banque n'a pas donné suite, nous pouvons recommander une indemnisation au motif que la banque n'a pas respecté ses engagements publics, comme le Code des cartes de débit, le Code des aînés et les propres documents de marketing de la banque concernant ses technologies de détection de la fraude. Cependant, dans les cas où des schémas discutables, mais pas manifestement frauduleux sont présents, nous ne pouvons pas recommander une indemnisation parce que les banques n'ont pas l'obligation de détecter ces schémas ni d'empêcher les transactions.

En prenant davantage de mesures pour prévenir activement la fraude, les banques maintiendraient et renforceraient la confiance des consommateurs dans le système financier. De plus, la prévention proactive des transactions frauduleuses réduirait l'incidence globale de la criminalité financière, ce qui rendrait le système financier plus sûr pour tous.

D'après notre expérience, les circonstances dans lesquelles la détection et la prévention devraient être requises comprennent les circonstances où :

- 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

Malgré la longueur et les détails de cette liste, la nature des activités frauduleuses change et évolue constamment à mesure que les criminels s'efforcent d'éviter tout mécanisme de détection qui a été mis au point pour les arrêter. La technologie utilisée par les banques pour détecter la fraude doit continuellement évoluer si l'on veut qu'elle reste efficace. Heureusement, les institutions financières au Canada et dans le monde ont une vaste expérience de l'identification et de la prévention des transactions frauduleuses, en particulier en ce qui concerne les produits de cartes de crédit. Nous nous attendons à ce que les institutions canadiennes soient en mesure de tirer parti de ces connaissances et de cette expertise pour aider à prévenir la fraude à l'égard d'autres produits et comptes bancaires.

Comme nous l'avons vu plus haut, il est probable que ces mécanismes de prévention de la fraude entraîneront un coût très important et que ces coûts seront en fin de compte intégrés au coût des produits et services bancaires pour tous les consommateurs. À notre avis, compte tenu des conséquences tout à fait dévastatrices des fraudes et des escroqueries pour les consommateurs touchés, les coûts des mécanismes de prévention, lorsqu'ils sont répartis entre tous les consommateurs des banques, sont appropriés dans les circonstances.

Exemple 3 – Hameçonnage des informations de compte

Mme V a reçu un message texte sur son téléphone mobile de ce qui semblait être l'un de ses fournisseurs de services mensuels. Selon l'aperçu du message, un crédit lui avait été remboursé. Pour en savoir plus, elle ouvre le message et clique sur le lien prévu à cet effet. Elle a ensuite été incitée à cliquer sur l'icône pour que sa banque poursuive le processus de remboursement et dépose le montant dans son compte bancaire. Son compte bancaire était lié à sa marge de crédit et à sa carte de crédit.

Après que Mme V a cliqué sur l'icône de sa banque, l'écran de son téléphone cellulaire a bogué pendant un moment. Son mari lui a conseillé de signaler l'incident à sa banque dès que possible et de savoir si l'un de leurs comptes avait été compromis. Elle a communiqué avec la banque, et le représentant lui a assuré qu'elle n'avait aucune raison de s'inquiéter. Plus tard dans la soirée, elle a reçu un avis confirmant qu'un virement électronique de 3 000 $ avait été accepté par un inconnu.

Exigence de désactiver les capacités du compte

QUESTION 2 : LES BANQUES DEVRAIENT-ELLES ÊTRE TENUES DE PERMETTRE AUX CONSOMMATEURS D'AVOIR LA POSSIBILITÉ DE DÉSACTIVER OU D'AJUSTER LES CAPACITÉS DE COMPTE POUR PRÉVENIR LA FRAUDE, COMME LA CAPACITÉ D'EFFECTUER DES VIREMENTS TÉLÉGRAPHIQUES?

Les consommateurs devraient avoir la possibilité de modifier les caractéristiques de leurs produits bancaires numériques de manière indépendante, en particulier toute fonctionnalité ayant la capacité de transférer des fonds à partir d'un compte. À notre avis, le fait de veiller à ce que les produits et services bancaires soient conçus pour intégrer un tel contrôle des consommateurs réduirait considérablement le risque de fraude des consommateurs en leur permettant d'activer uniquement les fonctionnalités dont ils ont besoin. Notre expérience a montré que de nombreux consommateurs ne sont pas conscients de la gamme complète des capacités de leurs services bancaires en ligne et des risques associés à ces services. Par exemple, la plupart des clients des banques canadiennes peuvent envoyer jusqu'à $50,000 par jour à l'échelle internationale grâce au transfert d'argent mondial disponible sur leur service bancaire en ligne. Dans de nombreux cas, nous avons constaté que les consommateurs n'avaient découvert cette fonctionnalité qu'après avoir été victimes de fraude et qu'un criminel avait transféré des sommes importantes de leurs comptes à des destinataires internationaux.

Nous reconnaissons que la capacité de transférer facilement des sommes importantes à l'échelle internationale est une caractéristique importante pour certains clients des banques canadiennes. Cependant, nous nous demandons si cette capacité est utile pour de nombreux Canadiens et s'ils choisiraient de l'activer, compte tenu de l'augmentation importante du risque de fraude qui y est associé.

Exemple 4 – Argent transféré à l'étranger

Mme A était une personne âgée aux moyens modestes qui a commencé à utiliser les services bancaires en ligne pendant la pandémie de COVID-19. Elle avait un petit montant dans son compte bancaire et avait une marge de crédit pour les urgences, qu'elle n'avait jamais utilisée. Un jour, elle s'est connectée à ses services bancaires en ligne et a vu que son compte bancaire était presque vide et que le solde de sa marge de crédit était supérieur à 20 000 $.

Sa banque lui a dit qu'une série de transactions avait eu lieu sur une période d'environ une semaine. Des sommes avaient été transférées de sa marge de crédit vers ses comptes bancaires, puis vers un destinataire dans un autre pays au moyen de la fonction Virement d'argent international de ses services bancaires en ligne. La banque a déclaré que chacune des transactions avait été autorisée par la saisie correcte d'un mot de passe à usage unique qui lui avait été envoyé. Mme A ne reconnaissait pas ces transactions, n'avait jamais utilisé Global Money Transfer et ne savait pas que de tels transferts étaient possibles.

Nous reconnaissons également que les banques sont sous pression concurrentielle et commerciale continue pour améliorer la facilité d'utilisation de leur expérience numérique des consommateurs. Cependant, à moins que la protection contre la fraude ne soit au cœur de la conception de nouveaux produits et services, les changements qui améliorent la convivialité peuvent également accroître considérablement la vulnérabilité des consommateurs à la fraude. C'est pourquoi il est crucial que les mesures de protection des consommateurs, y compris la capacité de refuser ou d'éliminer les caractéristiques du produit, soient une priorité.

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. L'établissement de processus d'identification améliorés pour la réactivation des fonctions du compte rendra le transfert à partir des comptes plus difficile pour les fraudeurs. Bien que cela rende également ces transferts plus difficiles pour les consommateurs, de tels inconvénients sont justifiables compte tenu des conséquences potentiellement dévastatrices de la fraude.

En outre, un choix éclairé sur l'opportunité d'activer des fonctionnalités avancées telles que le transfert d'argent mondial suppose toujours un niveau de sophistication que tous les consommateurs n'ont pas. Pour cette raison, toute nouvelle fonctionnalité qui augmente le risque de fraude d'un consommateur devrait par défaut ne pas être disponible et ne devrait être introduite que dans le cadre d'un programme complet et continu d'éducation des consommateurs.

Donner aux consommateurs le contrôle des capacités de leur compte numérique en leur permettant de désactiver ou d'ajuster les fonctionnalités et les limites en ligne peut réduire considérablement le risque de transactions non autorisées et de fraude et leur permettra de se protéger en adaptant les capacités de leur compte à leur tolérance au risque personnelle et à leurs habitudes d'utilisation.

De telles exigences peuvent également stimuler la concurrence et l'innovation entre les institutions financières pour être en mesure d'offrir des validations améliorées aussi facilement que possible.

Le fait de s'assurer que les banques offrent ces options de sécurité permettra d'accroître la confiance et la satisfaction des consommateurs, car les consommateurs sont plus susceptibles de se sentir en sécurité et en confiance dans leur relation bancaire, sachant qu'ils ont des outils pour protéger leurs actifs financiers.

Obligation de détecter la fraude

QUESTION 3 : LES BANQUES DEVRAIENT-ELLES ÊTRE TENUES D'INSTAURER DES POLITIQUES ET DES PROCÉDURES POUR DÉTECTER LES FRAUDES ET LES ESCROQUERIES ET EMPÊCHER LES CONSOMMATEURS D'ÊTRE VICTIMES ET, DANS L'AFFIRMATIVE, QUELLES POLITIQUES ET PROCÉDURES SERAIENT LES PLUS EFFICACES?

Comme il a été mentionné ci-dessus, la détection de la fraude est à la base de 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. Les consommateurs des banques, cependant, n'ont aucun moyen d'évaluer la qualité du programme de détection de la fraude d'une banque et ne peuvent donc pas choisir leur banque sur cette base, de sorte que les forces traditionnelles du marché ne peuvent pas être invoquées pour motiver les banques à investir des technologies de détection de fraude robustes.

Nous croyons que les banques canadiennes ont l'occasion d'investir dans la mise au point de systèmes améliorés de surveillance et de détection, y compris ceux qui analysent le comportement des consommateurs et détectent les tendances des transactions frauduleuses décrites ci-dessus d'une manière plus précise et cohérente et qu'il s'agit d'un domaine approprié pour l'établissement de normes réglementaires.

Exemple 5 – Aîné victime de fraudes répétées

M. H était un aîné qui détenait un compte chèques et une carte de crédit auprès de sa banque. Il avait déjà été victime d'une fraude en cryptomonnaie et avait perdu 26 000 $ en 2022. Un jour, il a accédé à son compte, a remarqué que le solde de son compte était bas et a vu que plusieurs virements électroniques non autorisés d'une valeur totale de 13 800 $ avaient été effectués de son compte chèques vers le même destinataire de cryptomonnaie que celui de la fraude précédente.

Il n'a pas reconnu le destinataire et ne pouvait pas se rappeler comment cette fraude a pu se produire. Il a signalé le problème à sa banque et celle-ci n'a offert aucune compensation.

Limites de responsabilité

QUESTION 4 : FAUDRAIT-IL INTRODUIRE UN SEUIL DE RESPONSABILITÉ MAXIMAL POUR LES TITULAIRES DE COMPTE QUI SONT VICTIMES DE TRANSACTIONS NON AUTORISÉES, SANS ÉGARD AUX MOYENS PAR LESQUELS ON A ACCÉDÉ À LEURS FONDS (PAR EXEMPLE, TRANSACTION PAR CARTE, VIREMENT TÉLÉGRAPHIQUE, TRANSFERT ÉLECTRONIQUE DE FONDS), ET SUR LES CIRCONSTANCES DANS LESQUELLES LES CONSOMMATRICES ET LES CONSOMMATEURS DEVRAIENT ÊTRE TENUS RESPONSABLES DE LA PERTE DE LEURS FONDS À LA SUITE DE TRANSACTIONS NON AUTORISÉES?

Les Canadiens et les banques canadiennes connaissent très bien les mesures de protection des consommateurs qui limitent leur responsabilité à l'égard des transactions frauduleuses. À l'heure actuelle, cette protection est en place pour les transactions par carte de crédit et de débit, mais elle n'est pas en place pour les autres transactions. Cet écart mène à la confusion et à la consternation lorsque les consommateurs constatent qu'ils ont perdu de l'argent de leur compte bancaire ou de leur ligne de crédit à la suite d'une fraude ou d'une arnaque et qu'ils ne sont pas protégés.

Notre expérience a montré que les attentes de nombreux consommateurs en matière de protection contre la fraude ne sont pas satisfaites et nous craignons que cela n'entraîne une érosion de la confiance des consommateurs. Cette attente des consommateurs se fonde probablement sur la compréhension générale et la publicité de protections de type « responsabilité zéro » pour les produits de cartes de crédit et sur la réputation que les banques canadiennes sont sûres et sécurisées pour les dépôts des consommateurs.

Pour certains consommateurs, cette attente de protection peut également résulter de l'expérience des pratiques de prévention de la fraude dans les banques qui détectent et préviennent certaines transactions suspectes, mais en passent à côté d'autres.

De plus, le libellé utilisé par les banques pour décrire leurs propres garanties contre les fraudes peut prêter à confusion, car il peut promettre une protection contre la fraude pourvu que le consommateur « protège » ses renseignements. Pour de nombreux consommateurs, le fait de cliquer par inadvertance sur un lien malveillant ou d'être trompés par un fraudeur ne constitue pas une incapacité à protéger leurs renseignements.

Exemple 6 – Une victime de fraude remet sa carte et son NIP à la « police »

M. J était un nouveau Canadien. Il a reçu un appel téléphonique qui semblait être de son service de police local. L'appelant a prétendu être policier et a informé M. J qu'il avait été victime d'une fraude bancaire et que sa carte avait été compromise. Le policier lui a dit qu'il devait saisir la carte bancaire de M. J pour l'utiliser comme preuve et a affirmé qu'un officier viendrait bientôt la récupérer chez lui. Lorsque l'agent s'est présenté à sa porte, M. J a remis sa carte et son NIP.

M. J a alors appelé sa banque pour signaler la situation et sa banque l'a informé qu'il avait été victime d'une escroquerie et a désactivé sa carte. Cependant, le fraudeur avait déjà retiré $2,500 du compte de M. J.

Nous croyons que les limites de responsabilité et les pratiques de détection et de prévention de la fraude actuellement appliquées aux cartes de crédit offrent un bon modèle pour d'autres produits et services bancaires. Les consommateurs bénéficient de protections générales lorsqu'ils utilisent leur carte de crédit, qui sont prévues par la Loi sur les banques, les lois provinciales sur la protection des consommateurs et les ententes avec les titulaires de carte. Par exemple, l'article 627.33 de la Loi sur les banques prévoit que le consommateur ne peut être tenu responsable d'une transaction non autorisée, sauf s'il y a eu de sa part négligence grave ou, au Québec, faute lourde, jusqu'à 50 $. Dans ces cas, il incombe à la banque de prouver que le consommateur a fait preuve de négligence grave.

Un régime de responsabilité normalisé serait plus facile à comprendre pour les consommateurs et inciterait clairement les banques à investir dans des stratégies appropriées de détection, de prévention et de protection de la fraude.

Bien que nous appuyions l'introduction d'un seuil de responsabilité comparable à celui des cartes de crédit, nous croyons également qu'il devrait faire partie d'une stratégie de prévention de la fraude plus vaste et plus complète pour le Canada qui reconnaît le rôle important que d'autres intervenants doivent jouer dans l'atteinte de cet objectif essentiel. Les principaux intervenants en matière de prévention de la fraude sont les suivants :

- Organismes d'application de la loi chargés de faire respecter les lois pénales
- Entreprises de télécommunications et de technologie dont les produits et services sont souvent impliqués dans la commission de fraudes
- Consommateurs qui ont la responsabilité ultime de se protéger, et de protéger leurs appareils et leurs renseignements des criminels.

Tous ces intervenants devraient participer à un vaste programme de prévention de la fraude pour la protection de tous les Canadiens.

Toutefois, cette consultation est axée sur le potentiel de prévention de la fraude du secteur bancaire et, comme décrit précédemment, nous sommes d'avis que le secteur pourrait en faire plus.

Si un seuil de responsabilité maximale pour les consommateurs était mis en œuvre, il est probable que cela inciterait fortement les banques à s'assurer que les systèmes de détection sont d'une robustesse et d'une exhaustivité optimales. C'est pourquoi un régime de responsabilité pourrait remplacer les obligations réglementaires distinctes qui consistent à détecter et à bloquer les transactions frauduleuses mentionnées précédemment. Au lieu d'une loi normative, un régime de responsabilité établirait des incitatifs financiers axés sur les résultats pour que les institutions élaborent et mettent en œuvre des mécanismes de détection et de prévention de la fraude de façon proactive.

Définition d'une transaction non autorisée

QUESTION 5 : QU'EST-CE QUI CONSTITUE UNE TRANSACTION NON AUTORISÉE ET COMMENT CES TRANSACTIONS DEVRAIENT-ELLES ÊTRE DÉFINIES?

Dans les cas de fraude et d'escroquerie, la distinction entre les transactions autorisées et non autorisées peut être floue. Il est clair que si la carte ou les informations

d’identification d’une personne lui sont volées, physiquement ou numériquement, et qu’elle n’est pas impliquée dans la transaction de quelque façon que ce soit, la transaction n’est pas autorisée. Cependant, il arrive à l'occasion que les consommateurs prennent part à une transaction qui ne correspond pas à l'image qu'ils s'en font. Par exemple, ils peuvent croire qu’ils envoient de l’argent dans un but légitime pour découvrir plus tard qu’ils avaient affaire à un fraudeur. Dans d'autres situations, un consommateur peut entrer ses coordonnées bancaires ou un mot de passe à usage unique, car il croit qu'il a affaire à la police ou à sa banque, et découvrir ultérieurement qu'il s'agissait d'un imposteur criminel. Dans ces situations, bien que le consommateur ait été personnellement impliqué dans la transaction, il n’a pas consenti aux caractéristiques essentielles de la transaction.

À notre avis, il faudrait définir l'autorisation comme des circonstances selon lesquelles un consommateur comprend les principales caractéristiques de la transaction, c'est-à-dire le montant qu'il transfère et la personne à qui il le transfère, et y donne son consentement de manière éclairée. La protection associée aux transactions non autorisées pourrait être assujettie au fait que le consommateur n’a pas fait preuve de négligence grave dans son traitement de ses renseignements confidentiels.

Exemple 7 – Coordonnées de compte volées

Mme B avait un compte chèques auprès de sa banque auquel elle accédait souvent par l’entremise des services bancaires en ligne. Un jour, Mme B. avait de la difficulté à se connecter à son compte bancaire en ligne et a reçu un message texte de ce qui semblait être sa banque. Elle a ouvert le message et a cliqué sur le lien fourni, ce qui l’a amenée à un site Web qui ressemblait à celui de sa banque, et elle a entré son numéro de carte de débit et son mot de passe. Peu de temps après, elle a découvert qu'un paiement de facture de 24 300 $ avait été effectué à partir de son compte.

Mme B s'est plainte que la banque aurait dû empêcher le paiement de la facture et lui a demandé un remboursement. La banque n’a pas accepté de rembourser parce qu’elle n’a pas protégé ses renseignements bancaires.

Nous croyons qu'une définition plus claire de ce qui constitue une autorisation permettra de préciser la responsabilité et d'accroître l'équité.

Exigences en matière de collecte de données

QUESTION 6 : LES BANQUES DEVRAIENT-ELLES ÊTRE TENUES DE RECUEILLIR ET DE DÉCLARER DES DONNÉES AGRÉGÉES ET ANONYMISÉES SUR LA NATURE DE LA FRAUDE ET DES ESCROQUERIES CIBLANT LEURS CLIENTS ET, DANS L'AFFIRMATIVE, LES BANQUES DEVRAIENT-ELLES ÊTRE TENUES DE DÉCLARER CES DONNÉES À L'ACFC?

Nous appuyons l'établissement d'une collecte de données agrégées à l'échelle du système sur les fraudes et les escroqueries, car cela améliorerait la détection des fraudes, l'identification des modèles et la possibilité de créer des stratégies de prévention efficaces fondées sur une expérience réelle.

Nous reconnaissons que le coût de la collecte, de l'agrégation et de l'analyse de ces données sera important. Toutefois, cet investissement serait justifié si les renseignements tirés des données recueillies étaient utilisés efficacement pour apporter des améliorations systémiques, améliorer les stratégies d'éducation et de prévention de la fraude et accroître la confiance des consommateurs.

Dans un tel système d'agrégation de données, l'ACFC doit s'assurer qu'il existe un mécanisme approprié pour la rétroaction des données et des renseignements clés à l'industrie, au public et à tout tiers fournisseur de services engagé dans la prévention et la détection de la fraude.

Exemple 8 – Informations d'identification bancaires utilisées pour une transaction inhabituelle

M. G détenait une marge de crédit hypothécaire auprès de sa banque et accédait souvent à ses comptes par l'entremise de l'application mobile de la banque. Il passait en revue ses comptes tous les mois.

Au cours de l'une de ses révisions mensuelles, il a constaté qu'un paiement de facture de 85 000 $ avait été envoyé de sa marge de crédit hypothécaire à un tiers qu'il ne reconnaissait pas. Il n'avait jamais fait de paiement de facture à partir de sa marge de crédit hypothécaire. Il a signalé la transaction non autorisée à sa banque et a demandé à la banque de rembourser le montant du paiement de la facture. La banque n'a pas accepté de rembourser M. G parce que ses renseignements bancaires ont été utilisés pour effectuer le paiement de la facture.

Thème 5 : Maintien d'une réglementation de calibre mondial

QUESTION 7 : LE MINISTÈRE DES FINANCES SOLLICITE DES POINTS DE VUE SUR LA PRÉVISIBILITÉ DE LA RÉGLEMENTATION ET SUR L'AMÉLIORATION DE LA COMPRÉHENSION DES MESURES ET DES RÉPERCUSSIONS RÉGLEMENTAIRES. CES DISPOSITIONS POURRAIENT COMPRENDRE :

- DES ANNONCES PÉRIODIQUES COORDONNÉES SUR LES MESURES RÉGLEMENTAIRES VRAISEMBLABLEMENT À VENIR;
- LA RÉALISATION ET LA PUBLICATION D'ÉNONCÉS DES RÉPERCUSSIONS SUR LES MESURES RÉGLEMENTAIRES;
- LA MISE EN PLACE D'UN FORUM POUR TRAVAILLER EN COORDINATION ET EN COLLABORATION SUR LES ENJEUX INTERNATIONAUX;
- L'ÉCHANGE DE RENSEIGNEMENTS SUR LES RISQUES MENAÇANT L'INTÉGRITÉ ET LA SÉCURITÉ.

Nous sommes d'accord avec les quatre dispositions proposées. L'OSBI travaille à l'intersection de la collaboration fédérale, provinciale et territoriale en ce qui concerne les services financiers et la protection des consommateurs. En plus de régler les différends au sein du secteur bancaire canadien, l'OSBI fournit des services d'ombudsman financier à presque toutes les firmes de courtage en valeurs mobilières sous réglementation provinciale (y compris les filiales de placement appartenant aux grandes banques canadiennes), ainsi qu'à de nombreuses caisses d'épargne et de crédit et à leurs membres.

Nous tenons souvent compte des lois et des règlements fédéraux et provinciaux dans notre travail de règlement des différends, y compris les lois provinciales sur la protection des consommateurs.

De notre point de vue, il est clair que de nombreuses distinctions historiques entre les « quatre piliers » des secteurs, des institutions et des produits distinctement réglementés s'estompent ou disparaissent complètement. Bien que les banques, les coopératives de crédit, les sociétés d'investissement et les compagnies d'assurance offrent des produits et des services distincts, il y a, de plus en plus, beaucoup de chevauchement dans leur conception, ainsi que dans les types de défis que les entreprises et les consommateurs rencontrent à leur égard. Cela correspond à un processus étendu et accéléré de consolidation et d'intégration au sein du secteur financier.

Les Canadiens ne connaissent généralement pas les structures réglementaires juridictionnelles qui sous-tendent la réglementation des produits et services financiers qu'ils utilisent au quotidien. Dans la mesure où la coordination et l'harmonisation entre les compétences provinciales et les administrations fédérales peuvent être améliorées, les consommateurs bénéficieront d'une plus grande uniformité et d'une plus grande prévisibilité des protections en place.

En ce qui concerne le premier point proposé dans le document de consultation, l'OSBI convient que des annonces périodiques coordonnées sur les mesures réglementaires vraisemblablement à venir seraient utiles et favoriseraient la sensibilisation et la transparence des entités réglementées et des organisations de consommateurs.

En ce qui concerne le deuxième point, nous appuyons la prémisse générale selon laquelle les répercussions probables de toute mesure réglementaire devraient être prises en compte avant la mise en œuvre. Toutefois, nous tenons à souligner que, pour que de telles répercussions soient adéquatement évaluées, il faudra veiller à ce que les entités réglementées et les groupes de consommateurs aient été sérieusement consultés. Nous avons observé que même si les entités réglementées et les organisations de l'industrie sont généralement bien placées pour évaluer les répercussions de la réglementation sur elles-mêmes et sur leurs intervenants, les groupes de consommateurs manquent souvent des ressources nécessaires pour présenter leur point de vue avec autant de rigueur. En plus de cette inégalité des ressources, la valeur des mesures de protection des investisseurs est souvent plus difficile à mesurer ou à quantifier que les coûts associés à la mise en œuvre. Comme solution possible à ce déséquilibre, le gouvernement fédéral, par l'entremise de l'ACFC, pourrait mandater des experts tiers pour évaluer ou directement mesurer les répercussions potentielles de toute mesure réglementaire proposée sur les consommateurs, éventuellement en collaboration avec les gouvernements provinciaux et territoriaux.

Sur le troisième point, nous sommes très favorables à la création d'un forum de coordination et de collaboration sur les questions internationales. Bon nombre des enjeux et des défis auxquels font face les décideurs canadiens sont partagés par les décideurs d'autres pays, et la coordination et la collaboration peuvent faciliter une plus grande efficacité et une meilleure prise de décisions. En outre, de nombreuses questions de politique générale auxquelles le secteur des services financiers est confronté ont une portée internationale et seraient mieux traitées par des réponses coordonnées à l'échelle internationale. Des défis tels que la lutte contre la fraude et d'autres crimes financiers, la réglementation efficace des entreprises de technologie financière dans le domaine bancaire axé sur les consommateurs et l'utilisation de l'intelligence artificielle dans le secteur des services financiers sont autant d'exemples de domaines qui tirent profit d'une coordination internationale.

En ce qui concerne le quatrième point, il est clair que la protection des consommateurs canadiens implique un chevauchement important des compétences entre le fédéral et divers organismes de réglementation provinciaux et territoriaux. D'après notre expérience, les différences dans les approches adoptées par les diverses provinces et le gouvernement fédéral sur les questions de protection des consommateurs peuvent entraîner de la confusion et des lacunes dans la protection. Nous avons observé que les entités sous réglementation fédérale qui exercent des activités dans l'ensemble des provinces ont parfois une connaissance limitée des règles provinciales de protection des consommateurs, et ce problème est aggravé par la divergence des approches en matière de protection financière pour les consommateurs d'une province à l'autre. Une plus grande harmonisation des règles de protection des consommateurs profiterait tant aux consommateurs qu'aux institutions, ce qui améliorerait la protection et la sensibilisation des consommateurs et des entités opérant dans l'ensemble des administrations. Nous tenons à constater qu'il existe déjà une harmonisation substantielle dans le secteur des valeurs mobilières, où les instruments nationaux utilisés par les organismes provinciaux de réglementation des valeurs mobilières profitent à la fois aux consommateurs et aux entités de valeurs mobilières opérant à l'échelle nationale. Une approche semblable à l'égard de la protection des consommateurs de produits et services financiers dans les secteurs des coopératives de crédit et des banques devrait être envisagée.

****

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