Prosper Canada

SOUMISSION AU MINISTÈRE DES FINANCES CANADA
Re : Réglementation relative à la fraude visant les consommateurs
22 décembre 2025

Introduction

Fondé en 1986, Prospérité Canada est un organisme de bienfaisance national qui est à l'origine de changements audacieux permettant à un plus grand nombre de personnes de prospérer. Nous travaillons en collaboration avec les gouvernements, les entreprises et les partenaires communautaires partout au Canada en étendant des services d'autonomisation financière qui changent des vies, en innovant pour une plus grande inclusion et un plus grand impact, et en éliminant les obstacles au bien-être financier des personnes ayant un faible revenu ou un revenu modeste. Notre objectif est de faire du Canada un pays où chaque personne a la possibilité et les moyens d'atteindre le bien-être financier et de vivre dans la dignité, la stabilité et l'épanouissement.

Les conclusions présentées ci-dessous s'appuient sur des données probantes et des observations recueillies dans le cadre de recherches et d'un dialogue continu avec les intervenants en matière de protection des consommateurs et nos partenaires communautaires partout au Canada. Ceux-ci travaillent directement avec les consommateurs ayant de faibles revenus et vulnérables sur le plan financier afin de les aider à renforcer leurs capacités financières, leur stabilité et leur bien-être. Cela implique notamment de leur donner les moyens de se protéger contre les abus financiers, les fraudes et les escroqueries, qui visent souvent les communautés ayant de faibles revenus, les communautés autochtones, les nouveaux arrivants, les personnes âgées et les personnes en situation de handicap.

Pour élaborer nos recommandations, nous avons pris en compte les facteurs suivants, en nous appuyant sur les renseignements et les données dont nous disposions :

- Preuves relatives au risque de fraude associé aux différentes fonctionnalités des comptes.
- Preuves de l'efficacité des mesures proposées pour réduire la fraude.
- Preuves de leur efficacité relative par rapport à d'autres mesures.
- Les implications opérationnelles des mesures proposées et leur potentiel d'augmentation des frais bancaires, des coûts ou des inconvénients pour les consommateurs.
- Alignement sur les pratiques efficaces établies en matière de transparence, de protection et d'autonomisation des consommateurs.

Nous nous réjouissons de pouvoir formuler des commentaires sur les règlements proposés et nous nous ferons un plaisir de répondre à toutes vos questions.

Réponse aux questions soulevées lors de la consultation

1. (a) Quelles fonctionnalités du compte devraient nécessiter le consentement exprès des consommateurs avant d'être activées?

Recommandations

Nous recommandons que les banques et les coopératives de crédit sous réglementation fédérale soient tenues d'obtenir le consentement exprès des clients pour effectuer des virements télégraphiques et des virements de fonds internationaux.

Nous recommandons que les banques et les coopératives de crédit sous réglementation fédérale continuent d'être tenues d'obtenir le consentement exprès des clients pour la protection contre les découverts.

Nous ne recommandons pas d'exiger un consentement exprès pour activer d'autres fonctionnalités du compte pour le moment, mais suggérons de les examiner à nouveau en tant qu'options à l'avenir, une fois que nous aurons acquis plus d'expérience en matière de mise en œuvre.

Justification

Étant donné que la protection contre les découverts est un produit de crédit, le consentement exprès du consommateur devrait toujours être requis avant d'activer cette fonctionnalité du compte. Cependant, comme le consentement exprès est déjà requis au Canada, il n'est pas nécessaire d'en faire une nouvelle exigence.

Les virements télégraphiques interbancaires et les virements de fonds internationaux sont les moyens de paiement préférés des fraudeurs, car ils sont généralement utilisés pour des transactions de grande valeur. En 2023, le Centre antifraude du Canada a indiqué que les virements télégraphiques interbancaires étaient le moyen de paiement ayant entraîné le plus de pertes financières, impliquant souvent des montants supérieurs à 10 000 dollars.

Une fois effectué, le virement de fonds effectué au moyen de ces mécanismes est généralement considéré comme définitif et irrévocable. Les criminels utilisent fréquemment les virements télégraphiques pour envoyer rapidement des fonds volés à l'étranger, ce qui rend la récupération de ces fonds extrêmement difficile, voire impossible dans de nombreux cas.

La plupart des consommateurs titulaires d'un compte de dépôt n'utilisent pas ces fonctions régulièrement, donc exiger leur consentement pour les activer ne représente pas un inconvénient pour la majorité d'entre eux. Selon une étude réalisée en 2024 par Paiements Canada, seulement 20 % des particuliers ont effectué des virements internationaux à partir de leur compte bancaire au cours d'une période de 12 mois. Parmi ceux-ci, les consommateurs étaient plus enclins à envoyer de l'argent à l'étranger en utilisant les TEF au moyen de leur application mobile de services bancaires ou de leur compte bancaire en ligne (31 %) et les virements PayPal (30 %). Les virements télégraphiques ont été utilisés par 11 % des consommateurs.

Nous estimons donc qu'il y a de bonnes raisons d'exiger des banques et des coopératives de crédit sous réglementation fédérale qu'elles obtiennent le consentement exprès de leurs clients pour activer les fonctionnalités de virement télégraphique et de virement de fonds internationaux. En effet, ce sont les types de virement que les fraudeurs sont les plus susceptibles d'utiliser pour voler des sommes importantes, les fonds virés sont en grande partie irrécupérables et la plupart des consommateurs n'ont pas besoin de ces fonctionnalités et ne les utilisent pas. L'authentification multifactorielle est généralement considérée comme le meilleur moyen de garantir que le « consentement exprès » provient bien du titulaire autorisé du compte.

Si cette approche est mise en œuvre, les banques devront réaliser des investissements dans les infrastructures et conserver les documents relatifs aux consentements à des fins d'audit. Cela pourrait entraîner une augmentation des frais pour les titulaires de comptes. Toutefois, si cette mesure permettait de réduire efficacement le risque de fraude et les pertes qui en découlent, les économies réalisées par les banques pourraient compenser les coûts opérationnels liés à la mise en place de cette protection, réduisant ainsi le risque de répercussion de ces coûts sur les consommateurs. Un suivi dans le temps permettra de mieux cerner l'impact de cette mesure.

Il est possible que les banques envisagent de désactiver par défaut certaines fonctionnalités supplémentaires des comptes pour les rendre « inactives sans consentement exprès » ou qu'elles soient tenues de le faire dans d'autres compétences dans le cadre de leurs mesures de lutte contre la fraude. Ces expérimentations doivent être suivies de près afin de fournir des renseignements précieux sur la rentabilité d'étendre cette approche à d'autres fonctionnalités du compte. Une fois que nous aurons acquis davantage d'expérience dans la mise en œuvre, le ministère des Finances Canada devrait examiner la pertinence de définir par défaut les autres fonctionnalités du compte comme « inactives sans consentement exprès ».

(b) Quelles fonctionnalités du compte les consommateurs devraient-ils être autorisés à désactiver?

Recommandations

Nous recommandons que les consommateurs soient autorisés à désactiver les virements télégraphiques et les virements de fonds internationaux en priorité, car (comme indiqué ci-dessus), ce sont les types de virement privilégiés par les fraudeurs qui causent les pertes financières les plus importantes. De plus, une fois ces virements effectués, ils sont généralement définitifs et irrévocables, ce qui rend le recouvrement des fonds difficile.

Il convient également d'envisager, à titre de priorité moyenne, de permettre aux consommateurs de désactiver les paiements de factures en ligne et d'autres transferts électroniques de fonds (TEF). Cela pourrait protéger une partie des personnes âgées et d'autres personnes qui préfèrent ne pas effectuer leurs opérations bancaires ou payer leurs factures en ligne, dans le cas où quelqu'un accèderait à leurs comptes sans autorisation. À condition qu'une authentification multifactorielle soit requise pour réactiver ces fonctionnalités. Toute tentative de réactivation d'une fonctionnalité désactivée doit également entraîner l'envoi d'une alerte au consommateur titulaire du compte.

Justification

Pour déterminer quelles fonctionnalités bancaires les consommateurs canadiens devraient avoir la possibilité de désactiver, il faut trouver un juste équilibre entre la sécurité, la commodité pour l'utilisateur et le profil de risque inhérent à chaque type de transaction. Les principales considérations sont les suivantes :

- **Gravité et irréversibilité de la fraude** : les fonctionnalités impliquant des sommes importantes et des transactions irréversibles présentent le risque le plus élevé.

- **Valeur et fréquence des transactions** : les fonctionnalités utilisées pour les transactions de grande valeur ou moins fréquentes (comme les virements télégraphiques) sont moins susceptibles de perturber la vie quotidienne si elles sont désactivées et offrent un gain de sécurité substantiel lorsqu'elles sont activées que pour une utilisation spécifique et vérifiée. Les fonctionnalités utilisées pour les transactions fréquentes, quotidiennes et de faible valeur (comme les transactions par communication en champ proche ou les TEF courants) sont très commodes. Les désactiver causerait probablement des inconvénients majeurs pour les transactions quotidiennes. Par conséquent, un simple bouton pour les activer ou les désactiver pourrait être moins pratique que d'autres

mesures, comme des limites quotidiennes ou un code NIP obligatoire pour certains montants.

- **Autres mesures de sécurité** : La disponibilité et l'efficacité des mesures de sécurité existantes, telles que l'authentification multifactorielle (AMF), la surveillance des transactions en temps réel et les politiques de responsabilité des consommateurs, doivent également être prises en compte. L'objectif est d'offrir aux consommateurs une option de désactivation afin de leur permettre de disposer d'un niveau de contrôle supplémentaire, en plus des protections par défaut mises en place par la banque. Cela leur donne les moyens de gérer leur propre tolérance au risque.

- **Contrôle et transparence pour les consommateurs** : Le Cadre de protection des consommateurs de produits et services financiers du Canada souligne l'importance de fournir des renseignements clairs et d'obtenir le consentement exprès des consommateurs pour les produits et services. L'option de désactiver certaines fonctionnalités permet aux consommateurs de gérer leur expérience bancaire en toute sécurité. Cependant, les banques doivent communiquer dans un langage clair les risques, les avantages et la manière dont ces fonctionnalités peuvent être facilement activées et désactivées.

En fin de compte, les fonctionnalités qui combinent un risque élevé de perte d'argent, une irréversibilité élevée et une faible fréquence d'utilisation devraient être considérées comme prioritaires pour l'ajout d'une option de désactivation contrôlée par l'utilisateur. Sur cette base, les virements télégraphiques et les virements de fonds internationaux sont hautement prioritaires pour l'ajout d'une option de désactivation en raison du risque élevé de fraude et du caractère définitif des transactions.

Les paiements de factures en ligne et autres TEF devraient être considérés comme une priorité moyenne en ce qui concerne l'ajout d'une option de désactivation. Bien que les TEF présentent généralement moins de risques au Canada pour chaque transaction et offrent davantage de protections ou de recours aux consommateurs, les montants élevés ou les comportements inhabituels peuvent tout de même être des indices de fraude. L'option de désactivation pourrait être utile pour les consommateurs très réticents à prendre des risques, et particulièrement pour ceux qui préfèrent ne pas effectuer d'opérations bancaires ou payer leurs factures en ligne.

Une partie importante des personnes âgées n'utilise pas les services bancaires en ligne et pourrait bénéficier d'une protection supplémentaire en ayant la possibilité de désactiver les TEF afin de se prémunir contre le vol en cas d'accès non autorisé à leurs comptes. Selon Statistique Canada, en 2022, 14 % des adultes âgés de 65 ans et plus n'avaient pas accès à Internet. Même les personnes âgées qui avaient accès à Internet étaient moins susceptibles

d'utiliser les services bancaires en ligne que les Canadiens plus jeunes, puisque seuls 76 % des internautes âgés de 65 à 74 ans utilisaient les services bancaires en ligne, tandis que les 24 % restants optaient pour des méthodes bancaires plus traditionnelles (p. ex. en succursale, par téléphone ou au guichet automatique) ou n'avaient pas de compte chèque ou d'épargne.

Les transactions par communication en champ proche ne sont pas une priorité en ce qui concerne l'ajout d'une option de désactivation, mais devraient être une priorité élevée pour d'autres mesures de sécurité, par exemple les limites de dépenses ou les exigences en matière de code NIP, en raison de leur utilisation fréquente dans les transactions quotidiennes de faible valeur.

Mise en œuvre d'une option permettant au consommateur de désactiver certaines fonctionnalités du compte

Les banques devraient donner aux titulaires de comptes la possibilité de désactiver et de réactiver facilement certaines fonctionnalités de leur compte à partir de leur portail bancaire en ligne, des applications mobiles ou en contactant directement la banque. Les consommateurs devraient pouvoir choisir le canal de communication qui leur convient le mieux et qui leur semble le plus pratique.

Les consommateurs devraient également être autorisés à modifier eux-mêmes les montants maximaux de leurs transactions quand ils le souhaitent, à partir des mêmes canaux, afin de se protéger contre d'éventuelles pertes liées à la fraude.

Les banques devraient également mettre en place des politiques et des procédures internes afin de gérer efficacement ces nouvelles options offertes aux consommateurs et fournir un processus de consentement clair à des fins d'audit.

Il est également recommandé aux banques d'adopter des lignes directrices en matière d'expérience utilisateur afin de garantir que tous les aspects liés au consentement et à la révocation soient clairs, simples et cohérents sur toutes les plateformes, conformément au nouveau cadre réglementaire pour les services bancaires axés sur le consommateur.

2. Comment les banques devraient-elles être tenues d'obtenir le « consentement exprès » des consommateurs afin d'activer certaines fonctionnalités de leurs comptes de dépôt personnels?

Recommandations

Les banques doivent obtenir le consentement exprès de leurs clients au moyen d'une communication claire, simple, concise et non trompeuse, indiquant explicitement qu'elles sollicitent leur consentement pour activer une fonctionnalité spécifique du compte.

Cette communication doit également inclure des renseignements clairs, simples, succincts et non trompeurs décrivant les éléments suivants :

- Les risques et avantages liés à l'activation de la fonctionnalité en question.
- Que le consommateur peut réduire le risque de fraude en n'activant aucune fonctionnalité dont il estime ne pas avoir besoin.
- Qui est responsable des pertes subies dans les cas suivants :
    - en cas d'accès non autorisé au compte et d'utilisation de cette fonctionnalité par une personne autre que le titulaire du compte;
    - si le titulaire du compte est victime d'une fraude et utilise lui-même la fonctionnalité pour virer des fonds à la partie frauduleuse.
- Comment les consommateurs peuvent retirer ou donner leur consentement à l'avenir s'ils le veulent.

Les consommateurs devraient être invités à donner leur consentement verbalement ou par écrit (y compris par voie électronique) au moyen du canal de communication de leur choix (par exemple, application mobile, site Web, en personne, par téléphone).

Une fois donné, le consentement doit être confirmé par écrit (par voie électronique ou sur papier) au titulaire du compte afin qu'il puisse en conserver lui-même une preuve permanente.

L'obtention du consentement pour activer des fonctionnalités à haut risque, telles que les virements télégraphiques et les virements de fonds internationaux, doit toujours inclure un processus de vérification en plusieurs étapes, tel qu'une vérification hors bande (par exemple, un code envoyé par SMS à un numéro de téléphone vérifié) afin de s'assurer que la personne qui donne son consentement est bien le titulaire du compte.

Les opérations à haut risque, telles que les virements télégraphiques et les virements de fonds internationaux, devraient également nécessiter un processus d'autorisation en plusieurs étapes pour chaque transaction spécifique afin de prévenir la fraude :

- Un accord écrit (y compris électronique) doit être en vigueur avant la première demande de virement. Cet accord doit préciser qui est autorisé à effectuer des virements, leurs coordonnées et les procédures de sécurité que la banque utilisera pour authentifier les demandes.

- L’accès aux systèmes bancaires utilisés pour effectuer des virements doit être protégé par des mots de passe forts et par une authentification multifactorielle.
- Il devrait y avoir un processus de vérification en plusieurs étapes pour les détails de la transaction. Cela pourrait impliquer un rappel direct vers un numéro de téléphone prédéterminé et vérifié qui figure déjà dans le dossier (et non un nouveau numéro ou un numéro différent fourni dans la demande de virement).
- Pour les opérations électroniques, un code numérique à usage unique envoyé par SMS au numéro de téléphone enregistré du client peut être utilisé comme moyen de vérification hors bande.

Pour chaque virement, le client doit fournir une autorisation explicite comprenant les éléments suivants :

- Nom du client et numéro de compte.
- Nom complet, adresse, nom de la banque et coordonnées bancaires du bénéficiaire (par exemple, IBAN, code SWIFT).
- Détails de la transaction : montant, devise et date du virement.
- Reconnaissance des frais associés ou du taux de change.
- Clause de non-responsabilité concernant les restrictions d’annulation.

Justification

Une communication claire, simple, concise et non trompeuse est essentielle pour permettre aux consommateurs de faire des choix éclairés qui servent au mieux leurs intérêts. Les déclarations longues et denses rédigées dans un langage juridique ne répondent pas à cette exigence. Les principaux renseignements doivent être communiqués dans un langage compréhensible pour toute personne ayant un niveau d’alphabétisation équivalent à celui d’un élève de 6^{e} année.

Les consommateurs doivent être informés des risques et des avantages liés à l’activation de la fonctionnalité du compte en question, car ces éléments sont nécessaires pour faire un choix éclairé et la plupart des consommateurs ne sont pas pleinement conscients des risques de fraude associés à certaines fonctionnalités particulières.

En informant les consommateurs qu’ils peuvent réduire le risque de fraude en n’activant pas les fonctionnalités de leur compte dont ils ne se servent pas ou sont peu susceptibles de se servir, on les aide à faire des choix prudents dans leur propre intérêt.

Il est essentiel de fournir des renseignements clairs indiquant qui est responsable des pertes liées au compte en cas d’accès non autorisé ou de virements effectués par le titulaire du compte à la suite d’une fraude ou d’une escroquerie. Sans ces renseignements, le

consommateur n'est pas en mesure d'évaluer pleinement les risques ni de faire un choix éclairé au sujet de la fonctionnalité en question.

Étant donné que la situation, la tolérance au risque et les besoins en matière de produits financiers des personnes évoluent, les consommateurs doivent savoir comment ils peuvent rapidement et facilement retirer leur consentement ou le donner à tout moment à l'avenir.

Un processus de consentement offrant une expérience utilisateur comparable sur tous les canaux de communication garantit que les banques ne créent pas involontairement des obstacles en matière d'accessibilité pour leurs clients, par exemple les personnes en situation de handicap, les clients qui n'ont pas accès aux technologies numériques ou qui ne savent pas les utiliser, les clients qui ont des difficultés liées à la distance ou à la mobilité, etc. Au contraire, elles permettent à chaque client de communiquer de la manière qui lui semble la plus facile et la plus pratique.

L'utilisation d'une authentification hors bande ou multifactorielle pour vérifier que la personne qui donne son consentement est bien le véritable titulaire du compte est une étape fondamentale qui protège les titulaires de compte dans le cas où quelqu'un aurait obtenu un accès non autorisé à leur compte et chercherait à activer des fonctionnalités à haut risque dans le but de commettre un vol ou une fraude.
En cas de fraude ou de perte de fonds liée à la fonctionnalité en question, il est essentiel que le titulaire du compte, tout comme la banque, dispose d'une preuve écrite claire (sur papier ou sous forme numérique) de tout consentement donné ou retiré en rapport avec cette fonctionnalité.

Pour les transactions à haut risque, telles que les virements télégraphiques et les virements de fonds internationaux, le consentement exprès doit aller au-delà de l'activation de la fonctionnalité et s'étendre à chaque transaction particulière afin de prévenir la fraude. Les canaux de paiement privilégiés par les fraudeurs nécessitent des niveaux de vérification supplémentaires afin de protéger adéquatement les consommateurs, en particulier lorsque, comme dans le cas présent, les fonctionnalités sont généralement utilisées pour des montants importants et que les paiements sont en grande partie irrévocables.

3. Y a-t-il d'autres limites que celles prévues au paragraphe 627.132(1) proposé que les consommateurs devraient pouvoir modifier?

Recommandations

Les limites proposées constituent un excellent point de départ, en particulier la limite du montant maximal des retraits et du nombre de retraits au cours d'une période donnée, car

cela permet aux consommateurs de limiter les pertes potentielles résultant d'un accès non autorisé à leur compte.

Pour que ces mesures soient efficaces, toute tentative de modification de ces limites doit entraîner une authentification multifactorielle afin de confirmer que la demande provient bien du titulaire du compte.

Voici d'autres limites que les consommateurs pourraient avoir intérêt à modifier :

- **Limites géographiques des transactions :** la possibilité de restreindre les lieux où les transactions peuvent être effectuées (par exemple, uniquement au Canada ou dans certaines provinces) peut aider à prévenir la fraude internationale ou interprovinciale si un client sait qu'il ne voyagera pas.

- **Limites par type de transaction :** les clients peuvent définir des limites pour certains types de transactions, par exemple en fixant une limite basse ou nulle pour les achats effectués en personne avec une carte de débit, s'ils utilisent principalement une carte de crédit pour ce type de transactions.

- **Limites spécifiques par commerçant ou catégorie :** la possibilité de bloquer les transactions provenant de certaines catégories de commerçants (par exemple, les jeux d'argent en ligne, les divertissements pour adultes) peut contribuer à prévenir la fraude dans des secteurs particuliers.

- **Limites horaires :** restreindre les heures auxquelles les transactions peuvent être effectuées (par exemple, aucune transaction entre minuit et 6 h du matin) pourrait contribuer à prévenir les activités frauduleuses qui se produisent souvent pendant la nuit.

- **Limites par transaction pour certains modes de paiement :** bien que des montants maximaux de retrait ou de virement soient proposés, des limites propres à chaque mode de paiement (par exemple, des limites différentes pour les virements électroniques et les prélèvements automatiques) pourraient offrir un meilleur contrôle.

- **Seuils d'alerte pour certaines activités spécifiques :** bien que des alertes de solde soient déjà exigées lorsque le solde d'un compte passe en dessous de 100 dollars (ou d'un montant défini par le client), permettre aux consommateurs de définir des alertes pour d'autres activités inhabituelles (par exemple, une transaction effectuée dans un nouvel endroit, une première transaction avec un nouveau commerçant, toute transaction dépassant un montant déterminé) permet de détecter les fraudes de manière proactive.

- **Fonction de verrouillage ou de gel temporaire :** la possibilité de verrouiller ou de geler instantanément certaines opérations d'un compte (par exemple, geler les transactions internationales en ligne tout en conservant les transactions nationales actives) en utilisant une application mobile, les services bancaires en ligne ou par téléphone, permettrait au client de se protéger immédiatement à la moindre suspicion d'utilisation frauduleuse.

La mise en œuvre devrait se faire progressivement, tout en surveillant son impact, car l'impact potentiel, l'effort opérationnel et l'investissement qui sont nécessaires à la mise en œuvre varieront selon les mesures. Cela contribuera à garantir un déploiement fluide, plus facile à gérer et efficace tant pour les institutions financières que pour les consommateurs.

La priorité doit être accordée aux mesures de contrôle faciles à mettre en œuvre à moindre coût et à celles qui offrent le plus grand potentiel de réduction du risque de fraude ou de limitation des pertes financières, même si leur mise en œuvre est plus coûteuse.

Justification

Ces mesures de contrôle donneraient aux consommateurs la possibilité d'adapter la sécurité de leur compte à leur mode de vie et à leur tolérance au risque, réduisant ainsi les pertes potentielles si les informations relatives à leur compte venaient à être compromises.

Dans d'autres pays, comme le Royaume-Uni, l'Australie et les États-Unis, certaines banques ont volontairement mis en œuvre certaines de ces mesures de contrôle, notamment en permettant aux consommateurs de bloquer les paiements à certaines catégories de commerçants et de geler ou débloquer leurs cartes. Ces fonctionnalités ne semblent pas être proposées par les banques canadiennes.

Nous ne sommes pas en mesure d'évaluer l'investissement opérationnel nécessaire pour mettre en œuvre ces mesures de contrôle supplémentaires destinées aux consommateurs. Néanmoins, il conviendrait de mesurer cet investissement par rapport à la réduction potentielle du risque de fraude et des pertes dans chaque cas afin de déterminer si la mesure de contrôle en question est rentable et devrait être mise en œuvre, puis de déterminer la priorité à lui accorder. L'évaluation des expériences pertinentes des banques dans d'autres compétences peut aider à recueillir des données et des conclusions importantes pour éclairer cette analyse.

4. La période minimale dont disposent les banques pour mettre en œuvre une modification de limite effectuée par le consommateur devrait-elle être fixée à 12 heures et la période maximale à 48 heures? Si ce n'est pas le cas, quelle devrait en être la durée?

Recommandations (avec justification)

Nous recommandons de fixer à 24 heures la période minimale pour mettre en œuvre une modification de limite afin d'augmenter les chances que le consommateur réfléchisse ou demande conseil s'il subit des pressions de la part d'une personne ayant l'intention de le frauder. Cela donne également plus de temps à l'institution financière pour intervenir pendant les heures d'ouverture afin de remettre en question les transactions suspectes.

Certains clients peuvent avoir des urgences légitimes nécessitant un accès plus rapide à des limites plus élevées. Pour répondre à cette situation, sans compromettre les mesures de prévention de la fraude, les institutions financières pourraient être autorisées à accélérer la modification après avoir vérifié l'identité du client et confirmé la légitimité de la demande grâce à une authentification renforcée. Ce processus d'authentification doit toutefois tenir compte du fait que l'une des fraudes les plus courantes consiste à utiliser l'intelligence artificielle pour imiter des membres de la famille en détresse demandant des transactions financières internationales urgentes, par exemple pour payer une caution, une rançon, etc. Les banques doivent établir un moyen fiable de distinguer les véritables urgences de ce type de fraudes, si elles font des exceptions à la période minimale de 24 heures.

Nous sommes d'accord avec la période maximale fixée à 48 heures, à condition que les institutions financières conservent le droit de la prolonger si elles détectent un risque de fraude et décident d'enquêter. Cela est essentiel pour que les banques puissent prendre des mesures en temps opportun afin de protéger les consommateurs et leurs propres institutions contre les pertes liées à la fraude.

5. Y a-t-il d'autres critères que ceux énoncés dans le paragraphe 627.134(2) proposé que les banques devraient inclure dans leurs politiques et procédures?

Recommandations

Nous recommandons d'ajouter les considérations suivantes dans les politiques et procédures bancaires régissant la détection, la prévention et les mesures d'atténuation des fraudes visant les consommateurs :

- Le délai dans lequel la décision de suspendre ou d'annuler une transaction doit être communiquée au consommateur.

- Les raisons pour lesquelles un consommateur peut contester une décision de suspendre ou d'annuler une transaction, et le processus par lequel la banque peut reconsidérer cette décision.

- Les délais dans lesquels une contestation peut être soulevée, la révision aura lieu et le consommateur doit recevoir une décision concernant sa contestation. Cela devrait permettre d'offrir une option de traitement accéléré prioritaire pour les cas où un préjudice financier réel est susceptible de se produire et où le temps est un facteur déterminant.

- Afin de réduire le risque de préjudice financier lié à la suspension de transactions légitimes, les banques devraient informer les consommateurs des types de transactions pour lesquelles ils doivent prévenir leur banque afin d'éviter tout retard et de garantir le bon déroulement de leurs opérations.

Justification

Les banques s'appuient souvent sur des algorithmes pour détecter les transactions potentiellement frauduleuses et prendre les mesures qui s'imposent, mais les algorithmes ne sont pas infaillibles. Lorsqu'un algorithme identifie à tort une transaction comme frauduleuse et qu'elle est refusée, cela peut nuire au consommateur et même causer un préjudice financier réel dans certains cas, par exemple en empêchant les consommateurs de respecter des délais de paiement importants ou en les mettant en défaut de paiement par rapport à leurs obligations contractuelles.

Les consommateurs devraient avoir la possibilité de contester ces décisions et d'obtenir une résolution rapide lorsque leur banque commet une erreur. En fournissant des directives claires sur les raisons valables pour contester une décision, le moment et la manière de le faire, ainsi que le délai dans lequel le consommateur peut s'attendre à recevoir une réponse, cela contribuera à garantir un processus de recours transparent, efficace et rapide.

Les banques peuvent aider les consommateurs à éviter les retards dans le traitement des transactions importantes en leur indiquant quels types de transactions sont généralement soumis à des délais de vérification et en les encourageant à prévenir leur banque lorsqu'ils prévoient d'effectuer une transaction importante susceptible d'être compromise, afin que celle-ci puisse être vérifiée au préalable par leur banque.

6. Quelles données les banques devraient-elles être tenues d'inclure dans le rapport annuel sur la fraude présenté au commissaire?

Recommandations (avec justification)

Nous recommandons que les banques soient tenues de consigner à la fois les cas de fraude et les tentatives de fraude afin d'évaluer leur taux de réussite dans la lutte contre les tentatives de fraude.
Les différences significatives entre les banques peuvent mettre en évidence les faiblesses de certaines approches qui doivent être corrigées ou les approches hautement efficaces en matière de prévention de la fraude qui doivent être plus largement diffusées et mises en œuvre.

Nous recommandons que la valeur des transactions frauduleuses soit consignée, car ces données peuvent être utilisées pour hiérarchiser les types de fraude les plus préjudiciables — pour les consommateurs et les banques — et orienter les efforts de prévention en conséquence.

7. Les données communiquées devraient-elles être segmentées par type d'autorisation frauduleuse (par exemple, transactions effectuées sous la contrainte ou transactions non autorisées)? Si oui, comment?

Recommandations

Nous recommandons de différencier les rapports sur les fraudes non autorisées visant les consommateurs et les fraudes résultant de transactions autorisées par un consommateur. Pour être efficace, la prévention peut nécessiter des approches très différentes dans chacun de ces cas. Il est donc important de comprendre les incidences relatives propres à chaque type et d'adapter et de cibler les stratégies de prévention en conséquence.

À notre avis, les transactions effectuées sous la contrainte ne devraient pas être considérées comme autorisées par le consommateur, car un consentement donné sous l'effet de la peur ou de l'intimidation n'est pas volontaire et ne constitue donc pas un véritable consentement.

L'ACFC devrait collaborer avec les banques et les organismes chargés de l'application de la loi afin d'élaborer une taxonomie différenciée pour les plaintes relatives à la fraude, ainsi qu'un système de codification associé que les banques pourraient utiliser pour permettre une

analyse plus détaillée des données relatives à la fraude et des efforts de prévention et d'application de la loi fondés sur des preuves.

Justification

Lorsque les clients signalent des transactions frauduleuses, les équipes d'enquête des banques les classent généralement en fonction de la méthode utilisée par le fraudeur et du niveau d'implication du client :

- **Transactions non autorisées :** Il s'agit de transactions que le consommateur n'a pas effectuées ou approuvées. En cas de coercition (par exemple, le client a été contraint de fournir son code NIP ou d'approuver un paiement), le client n'est pas considéré comme ayant « volontairement » autorisé la transaction. Les banques sont tenues d'examiner tous les facteurs pertinents, y compris si les circonstances échappaient au contrôle du titulaire de la carte, et ne doivent pas automatiquement tenir le client pour responsable simplement parce qu'une méthode d'authentification (comme un code NIP correct) a été utilisée.

- **Fraude par paiement initié par le payeur autorisé (PPA) (sans contrainte) :** Dans le cadre d'une fraude par PPA classique, le client est poussé à effectuer un paiement pour un fraudeur, mais n'agit généralement pas sous la contrainte directe ou la coercition impliquant une menace immédiate. La différence cruciale dans les rapports réside dans le fait que, dans de nombreuses compétences, les lois actuelles sur la protection des consommateurs offrent historiquement moins de protection en matière de responsabilité pour ce type de fraude, car le client a techniquement « autorisé » lui-même le paiement. Néanmoins, de nouvelles réglementations font leur apparition (comme au Royaume-Uni [en anglais seulement]) obligeant à rembourser les victimes admissibles.

- **Transactions effectuées sous la contrainte :** Ces opérations sont généralement considérées comme une forme de transaction non autorisée à des fins de responsabilité et de déclaration, car le consentement du client n'a pas été donné librement. En cas d'enquête, les autorités rechercheront des preuves de contrainte, d'intimidation ou de recours à la force.

Pour l'instant, les banques envoient tous les dossiers de plaintes de leurs clients à l'Agence de la consommation en matière financière du Canada (ACFC). D'après ce que nous comprenons, ces plaintes sont classées et la description de la « nature de la plainte » préciserait généralement les cas de coercition afin de permettre à l'organisme de réglementation d'identifier les tendances en la matière.

En travaillant en collaboration avec les banques et les organismes chargés de l'application de la loi afin d'élaborer une taxonomie plus différenciée des catégories de fraude, l'ACFC peut établir un système dans lequel les plaintes sont classées par catégorie spécifique de fraude, par exemple :

- **Carte non présente :** Vol en ligne
- **Carte présente** : Vol de carte physique
- **Ingénierie sociale ou fraude par PPA :** Le client se fait piéger et envoie de l'argent.
- **Contrainte ou coercition** : Le client est contraint d'effectuer la transaction.

Cette segmentation expresse garantit que l'analyse des données reflète la véritable nature du crime. En documentant les circonstances exactes de la fraude pendant l'enquête et en utilisant des codes de signalement internes et réglementaires détaillés, les banques peuvent segmenter efficacement ces données afin d'élaborer de meilleures mesures pour protéger les consommateurs et aider les organismes chargés de l'application de la loi.

8. Quand les banques devraient-elles être tenues de présenter un rapport annuel à l'ACFC (par exemple, après la fin de l'année civile ou de l'exercice financier de la banque)? Les rapports devraient-ils être harmonisés avec les autres rapports que les banques sont tenues de présenter (par exemple, rapport annuel sur les plaintes, rapports du conseil d'administration et des comités)?

Nous n'avons pas de recommandation à formuler à ce sujet, car nous ne sommes pas en mesure d'évaluer les implications opérationnelles et financières de ces deux options sur les banques. Il sera important d'adopter une approche cohérente en matière de présentation des rapports dans l'ensemble du secteur bancaire afin de faciliter l'analyse comparative et l'analyse des tendances.

9. Les institutions devraient-elles être tenues d'indiquer, lors de l'ouverture d'un compte de dépôt personnel, que certaines fonctionnalités ne seront pas activées sans consentement exprès et peuvent être désactivées, et que les limites de retrait et de virement peuvent être modifiées?

Recommandations (avec justification)

Oui, les institutions devraient être tenues de divulguer ces renseignements lors de l'ouverture d'un compte personnel afin que les consommateurs puissent décider s'ils veulent activer certaines fonctionnalités du compte et qu'ils puissent utiliser pleinement les options qui leur sont offertes pour choisir leurs propres limites de retrait et d'opérations.

Il est également important que les consommateurs sachent, dès l'ouverture du compte, qu'ils peuvent modifier ces paramètres à tout moment s'ils le veulent.

Conclusion

Nous vous remercions sincèrement d'avoir pris en considération notre point de vue sur ce sujet important. Si vous avez des questions ou si vous voulez discuter de l'une des recommandations ci-dessus, n'hésitez pas à communiquer avec :

Liz Mulholland
PDG, Prospérité Canada
lmulholland@prospercanada.org
Téléphone : 416 294-3373