CRPC | Chaire de recherche en prévention de la cybercriminalité

Notes *de synthèse*

Vol. 4, Num. 7
2024

Responsabilités en matière de fraude bancaire: étude de cas du Royaume-Uni et de l'Australie

Catherine Carpentier-Desjardins, candidate à la maîtrise en criminologie

Introduction

Alors que le volume des transactions bancaires réalisées en ligne ne cesse de croître, les cyberfraudes deviennent une préoccupation quotidienne grandissante pour les institutions financières et leurs clients, qu'il s'agisse d'entreprises ou de particuliers. Notamment, les fraudes dans lesquelles un individu est incité à effectuer une transaction vers un compte frauduleux sous divers prétextes, représenteraient environ 75% des cas de fraude [1]. D'ailleurs, selon INTERPOL [2], les stratagèmes les plus couramment utilisés en Amérique du nord pour tromper les individus sont les usurpations d'identité, les fausses relations amoureuses en ligne et les faux services d'assistance technique. Le terme **fraude par paiement « push » autorisé (APP)** est de plus en plus utilisé par le secteur bancaire pour englober ces fraudes sous un parapluie, car **elles impliquent l'autorisation volontaire du transfert de fonds par la victime** à la différence des fraudes où le malfaiteur accède au compte de sa victime pour y entreprendre des transactions malveillantes à son insu.

Bien que les banques se doivent de protéger les actifs de leurs clients de toute activité frauduleuse potentielle, il est aussi de leur devoir d'exécuter les opérations désirées et initiées par leur clientèle [3]. Ainsi, **il devient difficile de déterminer en cas de fraude APP, si les institutions financières ou les clients avaient pu être plus diligents, si l'une des parties est plus responsable que l'autre, et si les institutions financières devraient rembourser des victimes manipulées, mais ayant autorisé les transferts frauduleux**. Pour certains, il peut être facile de blâmer les victimes, car elles ne sont souvent pas perçues comme des victimes idéales. En ce sens, certains estiment que les victimes, de par leur implication dans des activités douteuses au moment de la victimisation, en fréquentant des plateformes de rencontre suspectes ou encore en cherchant des investissements à rendement élevé, ont joué un rôle déterminant dans la fraude en transférant leurs fonds [4]. D'autre part, le travail de détection et d'atténuation des fraudes mené par les banques n'est pas exempt de critique.

Cette note de synthèse porte donc sur la question épineuse de la responsabilisation et la déresponsabilisation des institutions financières et de leurs clients dans ces situations complexes. Cette question sera étudiée en abordant les cas du Royaume-Uni et de l'Australie, qui ont récemment pris des initiatives législatives et réglementaires afin d'augmenter le degré de responsabilité des institutions financières face à la fraude en ligne. Un survol des nouvelles mesures mises en œuvre sera proposé, ainsi qu'une analyse préliminaire de leurs avantages et limites.

Le Royaume-Uni

Avant de développer un cadre législatif et règlementaire innovant, le Royaume-Uni s'est concentré sur des stratégies alternatives ayant pour but de réduire les incidences de fraude, faciliter le traitement des cas de fraude et accompagner les victimes.

Action Fraud

Le lancement du **Centre national de signalement de la fraude et de la cybercriminalité *Action Fraud***, en octobre 2009, a fait de celui-ci un **point de référence pour les victimes en centralisant plusieurs ressources et procédures**. Le service est géré par la police de la ville de Londres, conjointement avec le *National Fraud Intelligence Bureau* (NFIB). **Les citoyens victimes de fraude peuvent émettre un signalement en ligne ou par téléphone à *Action Fraud*, signalement qui se traduit par la création d'un rapport officiel d'infraction, que le NFIB est chargé d'évaluer et d'acheminer à la force de police régionale appropriée pour la suite des procédures en matière d'enquête**. Le perfectionnement du système et la participation accrue des forces policières pour diriger les victimes vers le centre ont permis une augmentation significative des signalements. En 2013, les signalements via *Action Fraud* avaient augmenté de 17% par rapport à l'année précédente, suggérant un intérêt accru des victimes à dénoncer la fraude lorsqu'un système instaurant des procédures légales et fournissant des ressources d'accompagnement est mis à leur disposition.

Modèle de remboursement conditionnel

En mai 2019, **un premier modèle établissant des standards de sécurité et formulant des critères plus stricts de remboursement des fraudes par APP** est mis en place. Il s'agit du ***Contingent Reimbursement Model* (CRM)**, auquel les institutions financières peuvent adhérer sur une base volontaire. Bien que l'ensemble des banques et services de paiement ne soient pas signataires du code, **le CRM couvre approximativement 90% des fraudes APP du pays** [5]. Le code stipule qu'**il incombe aux institutions financières d'assurer le remboursement des fraudes APP, sauf si elles peuvent démontrer que le client victime n'a pas respecté leurs standards de sécurité** [6, 7]. Ainsi, les institutions émettrices et réceptrices des paiements partagent la responsabilité du remboursement, et le client assume la perte si la banque refuse de rembourser. Cette initiative fournit enfin un recours aux victimes, alors qu'un remboursement leur est garanti tant qu'elles suivent les règles de sécurité, par exemple ne pas ignorer un avertissement de la banque lors de la création de bénéficiaires ou l'initiation de transferts [6].

Parmi les avantages de ce système, on peut d'abord mentionner qu'**il incite les banques et services de paiements participants à bonifier leurs mesures de sécurité pour réduire leurs pertes dues aux remboursements**. D'ailleurs, l'implantation d'un système sur une base volontaire, avant de rendre quelques mesures quelle qu'elles soient obligatoires, accorde une période de transition et davantage de flexibilité aux institutions pour améliorer leurs pratiques. Également, **un système à participation volontaire est plus facile à modifier qu'une législation, permettant de corriger les défauts et obstacles rencontrés avant de rendre certaines mesures obligatoires**. Par exemple, à la fin avril 2023, toutes les institutions ayant adhéré au CRM devaient avoir mis en oeuvre la mesure de protection *Confirmation of Payee* (CoP). Cette mesure veut que les banques communiquent une demande aux clients afin que ces derniers confirment le nom de la personne bénéficiaire du compte vers lequel ils souhaitent envoyer des fonds, et ce, afin de détecter les cas de fraude APP [6].

Suite à l'implantation du CRM, le ***Financial Ombudsman* Service** (FOS) a observé **une aug-**

-mentation des plaintes pour des fraudes APP des clients d'institutions financières n'ayant pas signé le Code [5]. De plus, **le pourcentage de remboursements à la suite d'une fraude APP a augmenté de 25,4% en 2019 à 43,2% en 2020**. Certains remarquent cependant qu'il s'agit probablement d'**une hausse encore insuffisante, considérant qu'un remboursement devrait être garanti pour toute victime ayant suivi les procédures**. En effet, le désintérêt des institutions financières et le manque d'uniformité de l'application du Code ont été pointés du doigt, alors que certaines banques présentaient des taux de remboursement très inférieurs et que plusieurs semblaient exploiter la mesure de communication d'avertissement pour s'exempter du devoir de remboursement [6]. Finalement, à la vue de l'impact pratique limité de ce code volontaire, le besoin d'un modèle aux fondements législatifs plus robustes et aux obligations plus contraignantes a été discuté.

Stratégie nationale de lutte contre la fraude

En juin 2023, alors que **la fraude représente 40% de la criminalité, mais que seulement 1% des ressources policières y est alloué**, le pays adopte la ***Stratégie nationale de lutte contre la fraude***, visant à s'attaquer directement aux fraudeurs [8]. La stratégie se résume à **trois objectifs** : **poursuivre les fraudeurs**, **bloquer la fraude**, et **outiller la population**. À travers cette stratégie, **la création de la *National Fraud Squad* (NFS)** composée de plus de 400 enquêteurs spécialisés, contribuera à identifier et arrêter plus de fraudeurs. La stratégie compte également permettre **la bonification d'*Action Fraud***, **le changement des lois pour que davantage de victimes soient indemnisées**, et **la publication des informations sur les niveaux de fraude observés sur différentes plateformes** afin d'inciter les entreprises à participer à la lutte contre la fraude. D'autres mesures sont prévues, comme l'**interdiction des appels à froid (*cold calls*)*** sur tous les produits financiers pour limiter l'achat d'investissements frauduleux, et l'**interdiction des « fermes de cartes SIM »** (*SIM farms*)** pour contrer la tactique de l'envoi simultané de milliers de SMS frauduleux [8].

Nouveau modèle de remboursement

La dernière mesure d'envergure, dont la version finale a été publiée en décembre 2023 par le ***Payment Systems Regulator*** (PSR) britannique, indique qu'**il sera, à partir du 7 octobre 2024, obligatoire pour les institutions financières et systèmes de paiement de rembourser les victimes de fraude APP, sauf en de rares exceptions** [11]. Cette mesure sera imposée sur le *Faster Payments system* (FPS)*** où la majorité des fraudes se produisent [11]. Ainsi, cette norme viendra remplacer le CRM volontaire présentement en vigueur. Selon cette nouvelle approche, **les institutions émettrices et réceptrices de la transaction frauduleuse devront chacune couvrir la moitié des pertes**, et l'institution réceptrice sera responsable d'enquêter sur le cas et prendre une décision quant au remboursement dans un délai maximal de 35 jours ouvrables [14, 15].

---

* Un appel à froid consiste en un vendeur contactant un acheteur potentiel, sans que celui-ci n'ait sollicité cette prise de contact, et sans qu'il n'existe un lien préalable entre les parties [9] . Le Financial Guidance and Claims Act 2018 du Royaume-Uni a déjà banni les appels à froid pour les sociétés de dommages corporels et les prestataires de retraite, mais compte élargir cette interdiction à la vente de produits financiers [8].

** Les fermes de cartes SIM, hébergent, au moyen d'équipements spécialisés, un volume important de cartes SIM, lesquelles sont nécessaires pour acheminer des appels et envoyer des messages via le réseau cellulaire. L'équipement permet le fonctionnement et la gestion simultanés des cartes SIM à des fin de communication automatisées à grande échelle. En lien avec la fraude, ces fermes peuvent pratiquer des activités de messagerie frauduleuse de masse et contourner les tarifs lors d'appels frauduleux internationaux en utilisant des cartes SIM locales [8, 10].

*** FSP est un système de paiement électronique facilitant les transferts d'argent rapides et sécurisés, accessible aux titulaires de comptes bancaires au Royaume-Uni des banques participantes [12]. FSP est comparable au système canadien Interac e-transfert, avec une rapidité accrue et des limites de transfert moins restrictives [13].

Les victimes pourront réclamer le remboursement d'un montant jusqu'à concurrence de 415 000 £ (environ 719 112$ CA) un montant limite supérieur à celui de la perte financière moyenne des victimes de fraude APP en 2022 (2 340 £ [environ 4 055$ CA]) [5, 14, 15]. Les institutions pourront également imposer, à leur discrétion, une franchise de réclamation pouvant aller jusqu'à 100 £ (environ 173$ CA) [5]. Encore une fois, le modèle prévoit la possibilité d'un refus de remboursement, mais beaucoup plus strict que le CRM. En effet, **les institutions pourront refuser un remboursement seulement si elles peuvent prouver par prépondérance de probabilités une négligence grave de la part du client**. Entre autres, **il sera attendu des clients qu'ils se soumettent à une norme de diligence englobant trois éléments** : 1) **l'obligation de ne pas ignorer les avertissements**, 2) **l'exigence de notification rapide**, et 3) **l'exigence de partage d'information** [16]. Les clients doivent donc réagir aux avertissements de tentatives suspectées de fraude APP pour tenter de prévenir la fraude, informer leur banque de la fraude dans un délai raisonnable (13 mois) et communiquer toutes informations raisonnables requises par la banque pour examiner la réclamation [5, 16]. **Seul le manquement à une seule ou plusieurs de ces attentes pourra être considérées comme une négligence grave et entraîner un refus de remboursement**. Les banques ne pourront pas évoquer ou exiger le manquement à d'autres actions de la part des clients pour justifier un refus de remboursement. Ainsi, **l'objectif annoncé du PSR est qu'environ 95% des pertes de fraude APP soient remboursées grâce au nouveau modèle** [17].

Le modèle prévoit également **des protections supplémentaires pour les clients identifiés comme étant vulnérables**. Le PSR ne définit pas directement quels clients sont considérés comme étant vulnérables, mais renvoie les institutions financières aux lignes directrices du rapport du *Financial Conduct Authority* (FCA) de 2021 qui porte sur le traitement équitable de la clientèle vulnérable [17, 18, 19]. Le FCA offre une définition de clientèle vulnérable* assez large, fondée sur plusieurs caractéristiques regroupées sous **quatre facteurs de vulnérabilité** : **la santé**, **les évènements de vie**, **la résilience** et **la capacité du client** [20]. Ainsi, quelques exemples de caractéristiques de vulnérabilité sont les problèmes de santé physique ou mentale, les évènements de vie tels qu'un divorce ou un cas de violence conjugale, et d'autres facteurs comme le surendettement, la faible littératie financière et les difficultés d'apprentissage représentent des caractéristiques de clientèles vulnérables. Il est à noter que le sexe et l'âge ne sont font pas partie des caractéristiques de vulnérabilité. Ainsi, le PSR et le FCA s'attendent à ce que les institutions financières évaluent les fraudes au cas par cas afin de déterminer si le client présente des caractéristiques de vulnérabilité temporaires ou durables ayant contribué à sa victimisation [18, 19]. Cette tâche s'annonce hasardeuse, puisque **le FCA ne détermine pas un nombre de caractéristiques requises pour être considéré comme étant un client vulnérable, ce qui accorde un certain pouvoir discrétionnaire aux institutions financières**. De plus, certains enjeux quant à l'étiquetage de la clientèle sont soulevés, alors qu'un client ne se considérant pas comme étant une personne vulnérable pourrait se sentir discriminé d'être catégorisé ainsi [20].

En cas de fraude APP, **lorsqu'un client victime est considéré comme étant vulnérable, un remboursement ne pourra pas lui être refusé pour cause de négligence, et il n'aura pas à payer de franchises de réclamation** [14, 15]. Le PSR estime que cette approche est juste, car elle responsabilise suffisamment les clients en les encourageant à être diligents, mais leur assure simultanément une protection financière plus robuste lorsque des caractéristiques de vulnérabilité ont contribué à la fraude.

---

* « Un client vulnérable est quelqu'un qui, en raison de sa situation personnelle, est particulièrement susceptible d'être lésée, en particulier lorsqu'une entreprise n'agit pas avec les niveaux appropriés de soins ».

La responsabilisation des facilitateurs

Bien que la régulation du secteur financier soit centrale à l'approche du Royaume-Uni, il faut noter que **le pays reconnait parallèlement l'importance de responsabiliser d'autres institutions susceptibles de faciliter la commission de fraudes APP**. Par exemple, la ***Online Fraud Charter***, mise à jour en novembre 2023, invite les diverses entreprises œuvrant dans le secteur de la technologie, comme les plateformes de médias sociaux et les opérateurs de télécommunications, à démontrer publiquement leur volonté de collaborer avec le gouvernement britannique pour lutter contre la fraude [21]. **Les signataires de la Charte doivent, entre autres, adhérer à certaines normes quant au signalement, blocage et suppression de contenus frauduleux, ainsi que favoriser le partage de renseignements, et bonifier la transparence quant aux risques de fraude et aux protections offertes sur leur plateforme** [21]. De façon générale, cette charte représente une opportunité pour les acteurs du secteur des technologies de démontrer à la population et au gouvernement qu'ils sont conscients du risque d'exploitation financière facilité par leurs plateformes. Étant sur une base volontaire, la charte permet aux entreprises, au même titre que le CRM l'a fait, d'agir de façon autonome et de prendre conscience des normes désirées par le gouvernement avant que ces mesures ne deviennent obligatoires et contraignantes [21].

De plus, bien qu'il ne soit pas exclusif aux enjeux de fraude, le ***Online Safety Act***, publié en octobre 2023, renforcera la responsabilité des plateformes de médias sociaux et moteurs de recherche quant à la sécurité des utilisateurs. **Cette loi imposera à partir du printemps 2025, une série d'obligations aux fournisseurs de services en ligne (même ceux non basés au Royaume-Uni)**, sous peine de sanctions comme des ordonnances de restriction de service ou encore des amendes pouvant s'élever jusqu'à 18 M£ (environ 31 M$ CAD) ou 10% du chiffre d'affaires annuel mondial de l'entreprise [22].

Via une liste de délits prioritaires, incluant la fraude, **la loi oblige les plateformes à prendre des mesures robustes, non seulement pour supprimer tout contenu illégal, mais également pour les empêcher d'apparaître**. Les plateformes seront catégorisées selon leur ampleur, leur niveau de risque et la probabilité que des enfants y accèdent, et devront ensuite se plier aux exigences relatives à leur catégorie [22]. Au-delà des particularités pouvant varier d'une catégorie à l'autre, **la loi incite fortement les fournisseurs à revoir les impacts néfastes que leurs algorithmes pourraient avoir sur leur clientèle**, et pourrait exiger des rapports de transparence quant à la sécurité des plateformes [23].

En résumé, **le Royaume-Uni a, au fil des ans, transféré le fardeau financier des fraudes APP du consommateur vers les institutions**. Ainsi, les régulateurs britanniques veillent indirectement à ce que les prestataires financiers mettent en place des mesures de sécurité appropriées contre la fraude.

L'Australie

De son côté, **l'Australie est plus conservatrice dans son approche**, alors que **le pays mise davantage sur le développement et l'implantation de mesures de sécurité durables au sein du secteur financier plutôt que sur la réglementation pour répondre à la problématique de la fraude en ligne**. Également, **le pays ne prend pas position quant aux enjeux de responsabilité et de modalité de remboursement**. Les initiatives pertinentes pour soutenir les victimes et outiller les institutions financières qui ont été mises en place sont présentées ci-dessous.

IDCARE

En 2014, **IDCARE**, le service national d'identité et de cyberassistance de l'Australie et de la Nouvelle-Zélande voit le jour. Ce centre est un organisme à but non lucratif visant à combler le manque de soutien auquel sont confrontées les

victimes de vol d'identité et de cybersécurité. **IDCARE traite plusieurs formes de victimisations**, dont les fraudes téléphoniques, amoureuses, d'investissements et autres. **Les victimes sont mises en contact avec un expert qui leur fournit des conseils sur les mesures à prendre afin de faire face à leur situation**. L'organisation maintient également une bibliothèque « clé en main », regroupant des milliers des mesures spécifiques et plans d'intervention pouvant éduquer les victimes et les aider à répondre à leur situation. **IDCARE a répondu à plus de 100 000 cas depuis 2014, et continue d'être soutenue financièrement par plus de 45 entités**, dont plusieurs départements du gouvernement australien, corps policiers, institutions financières, universités et autres organismes, tels qu'Equifax. D'ailleurs, en 2022, 2 M$ AU (1 841 800$ CA) ont été alloués au au ministère de l'Intérieur australien afin d'élargir son partenariat avec IDCARE, notamment en permettant à l'organisme de fournir des services spécialisés tels que des services de conseils et de récupération d'identité pour les victimes de vol d'identité [24].

National Anti-Scam Centre

En avril 2023, l'autorité régulatrice des entreprises, des marchés et des services financiers, l'***Australian Securities and Investments Commission*** (ASIC), publie un rapport dont les constats mettent en lumière les enjeux auxquels le système financier fait face en matière de fraude. En effet, **après avoir analysé les stratégies antifraude de quatre grandes banques australiennes, le rapport déplore que ces dernières aient de faibles capacités à prévenir, perturber et répondre aux activités frauduleuses** [3]. Notamment, il en ressort que **dans la majorité des cas (96%), les clients sont perdants financièrement, alors que les banques détectent et remboursent très peu les transactions frauduleuses**. Collectivement, les quatre banques auraient détecté et empêché seulement 13% des transactions frauduleuses de leur clientèle et les taux de remboursement varient de 2 à 5% [3]. Le rapport fait également mention de l'hétérogénéité des mesures de sécurité et de détection de transactions frauduleuses au sein des institutions financières. L'efficacité des mesures serait également variable. De manière générale, **le rapport démontre un besoin criant d'harmonisation des pratiques de sécurité et de leur efficacité à travers les acteurs du système financier**.

Peu de temps après la parution du rapport de l'ASIC, en mai 2023, le gouvernement fédéral annonce la création du ***National Anti-Scam Centre*** auprès de l'***Australian Competition and Consumer Commission*** (ACCC) [3]. Établi en juillet 2023, le centre, cordonné par le gouvernement et les forces de l'ordre, vise à la fois à **bonifier le partage de renseignement portant sur les cas de fraude**, et à **sensibiliser la population à la problématique**. Entre autres, le centre a mis en ligne la plateforme ***ScamWatch***, sur laquelle les individus peuvent signaler une fraude. Bien que ces rapports ne soient pas utilisés à des fins d'enquêtes, ils sont utilisés par le centre pour identifier les nouvelles fraudes et les tendances, développer des stratégies et avertir la population. Le centre réfère les individus à IDCARE ainsi qu'à leur institution financière pour obtenir de l'assistance, et indique également qu'un signalement officiel à la police peut être soumis en ligne via la plateforme du ***Australian Signals Directorate***. Malgré la création du centre, il n'existe toujours pas de cadre réglementaire global clarifiant les rôles et les responsabilités du gouvernement fédéral, des organismes régulateurs et du secteur privé en matière de fraude.

Scam-Safe Accord

La mesure la plus récente visant à rehausser plus directement les mesures de sécurité et de détection de transactions frauduleuses des banques a été annoncée en novembre 2023 par l'***Australian Banking Association*** (ABA). Le *Scam-Safe Accord* résulte d'une collaboration des acteurs du secteur bancaire qui s'engagent,

au cours de l'année 2024 et des années qui suivront, à adopter plusieurs mesures antifraude [25]. Les mesures couvrent **trois éléments clés de la lutte à la fraude**, soit **la détection**, **l'interruption** et **la réponse**. Parmi les mesures adoptées, les institutions adhérant à l'accord devront investir 100 M$ AU (environ 73 M$ CA) pour le déploiement d'un système de confirmation du bénéficiaire, tel que le *CoP* déployé au Royaume-Uni. Également, elles devront se joindre à l'***Australian Financial Crimes Exchange*** (AFCX) dans le but d'**accroître le partage de renseignement entre institutions**. Finalement, elles devront introduire certaines pratiques comme l'envoi d'avertissements aux victimes potentielles lors d'un transfert de fonds à un nouveau bénéficiaire, et des délais de transactions accrus pour permettre une vérification rigoureuse de la légitimité des transferts et des nouveaux bénéficiaires [25]. Le ministre du Trésor australien s'est réjoui de cet accord, et a déclaré que les institutions participantes prenaient de l'avance sur les réglementations prévues prochainement par le gouvernement [26]. En effet, **le gouvernement travaille sur de nouveaux règlements industriels stricts, tant pour les banques, que les opérateurs de télécommunications et les plateformes numériques comme les médias sociaux**. Ces règlements devraient rendre obligatoires certaines mesures afin de protéger les citoyens telles que la collaboration avec les entreprises de télécommunications pour bloquer les messages texte frauduleux.

Les efforts communs des acteurs du secteur financier sont sans doute prometteurs pour lutter contre la fraude. Toutefois, il n'en est pas moins que, **même si la bonification des mesures de protection de la clientèle risque de diminuer les incidences de fraude, aucune mesure concrète de recouvrement des fonds n'est envisagée pour ceux qui seront victimisés**. La position de l'Australie quant à la responsabilisation des clients demeure donc incomplète.

Avantages, inconvénients et défis des approches

Enjeux liés au remboursement et au niveau de diligence attendu des clients

Globalement, on peut conclure que **l'approche du Royaume-Uni, reposants sur une législation et des mesures strictes de remboursement, est plutôt réactive face aux cas de fraude, tandis que celle de l'Australie s'inscrit plutôt dans une perspective préventive, alors qu'elle mise sur la restructuration des pratiques de sécurité du secteur bancaire pour diminuer les incidences de fraude**. Dans les deux cas, les approches se heurtent à des défis de mise en œuvre et des inconvénients. Par exemple, en refusant de rembourser seulement les victimes ayant fait preuve de négligence grave, on peut penser que l'approche du Royaume-Uni déresponsabilise trop les clients en diminuant leur incitation à la diligence et à la vigilance lors d'opérations bancaires en ligne. D'ailleurs, plusieurs organismes professionnels et groupes industriels ont critiqué l'approche du PSR quant à la négligence grave, suggérant qu'une norme de diligence pas assez stricte pourrait augmenter la fraude [18, 19]. Ils avaient également, au même titre que les signataires du CRM, déploré **le manque de précision quant à la définition du concept de négligence grave**, chose que le PSR a rectifié la situation en 2023 en ajoutant les trois normes de diligence du client (réaction aux avertissements, notification rapide et partage d'information), des éléments observables et mesurables permettant d'établir si le client a été proactif face à la victimisation.

D'autre part, en ne déterminant pas de conditions d'admissibilité aux remboursements par les institutions bancaires, **l'Australie n'offre pas de filet de secours financier aux victimes, même pour la clientèle plus vulnérable**. Évidemment, l'approche du Royaume-Uni s'accompagne d'un important inconvénient, puisque les virements bancaires pourraient être

retardés jusqu'à quatre jours pour permettre aux banques de mener une enquête appropriée et de contacter la victime potentielle si une fraude est suspectée [27]. Il faut donc noter que **cette approche drastique introduit un défi de taille : concilier innovation et sécurité**. En effet, les délais représentent un pas en arrière par rapport au développement de systèmes de paiement rapide. Également, puisque les banques sont dans l'obligation de rembourser, certaines d'entre elles envisagent de renoncer aux paiements instantanés [27]. D'autres retombées négatives, comme l'entrave à l'innovation et la diminution des investissements internationaux sur le marché britannique sont craintes par différents membres de l'industrie [18, 19]

Enjeux économiques liés à l'implémentation

Il est difficile de quantifier les coûts supplémentaires qu'engendreront les remboursements obligatoires pour une institution financière, puisqu'ils varieront en fonction du taux de fraude que l'institution rembourse déjà dans le cadre des régimes volontaires actuels [28]. Les taux de remboursement sont actuellement nettement plus élevés dans les grandes banques, alors que la nouvelle réglementation risque d'être plus coûteuse et plus difficile à respecter pour les petites entreprises n'ayant pas préalablement adhéré au CRM et disposant de moins de capital [29]. **Pour réduire les coûts de la fraude, les banques devront miser davantage sur la prévention, mais l'implémentation des mesures nécessaires sera également coûteuse**. Entre autres, les banques devront concevoir des systèmes d'avertissement de tentatives de fraude, des systèmes pour traiter les demandes de remboursement, et garder une trace des indicateurs permettant d'évaluer le respect de la norme de diligence du client [30]. De plus, des formations risquent d'être nécessaires pour le personnel impliqué dans le traitement des réclamations et l'identification de la clientèle vulnérable [30]. Encore une fois, les coûts à prévoir en lien avec ces mesures sont flous, cela est d'ailleurs critiqué par plusieurs fir-mes qui notent le manque de quantification des coûts et avantages pertinents dans l'analyse coût-avantages publiée par le PSR [19]. Par exemple, dans la section des investissements requis de la part des institutions financières, le PSR ne fournit pas de chiffres, mais indique simplement que **l'investissement devrait être proportionnel à l'ampleur du problème de fraude de l'institution**. D'autres sections sont plus détaillées, par exemple le PSR estime que les frais administratifs d'enquête, de retard des paiements et de résolution des litiges pourraient totaliser de 17 M£ (environ 29 380 000$ CA) à 38 M£ (environ 65 670 500$ CA) annuellement pour l'industrie. Individuellement, les grandes banques (recevant plus de 10 M£ [environ 17 280 920$ CA] en fraude) devraient s'attendre à dépenser approximativement 2,1 M£ (environ 3 630 990$ CA) en frais administratifs, et celles recevant entre 500 000£ (environ 864 050$ CA) et 1 M£ (environ 1 730 090$ CA) devraient débourser environ 71 000£ (environ 122 695$ CA).

Enjeux liés à la réglementation

Quant aux réglementations, l'avis des experts est mitigé. D'un côté, **certains indiquent que la régulation freine l'innovation des services de paiements rapide, ce qui peut conférer un avantage technologique aux fraudeurs qui développent sans cesse de nouveaux modus operandi et mesures de contournement des systèmes en place** [27]. Ainsi, ils prônent l'innovation plutôt que la régulation, notamment avec l'usage de l'intelligence artificielle (IA) pour répondre au fléau de la fraude. À l'inverse, **l'absence de régulation peut devenir problématique, car les institutions n'ont pas d'incitatifs à investir des ressources pour lutter contre la fraude**. Similairement, les initiatives qui demeurent sur une base volontaire peuvent s'avérer inefficaces en l'absence d'incitatifs, car l'application pratique d'un modèle de ce genre risque d'être moins rigoureuse que celle d'un modèle obligatoire [6, 31].

Malgré leurs différences, ces deux approches démontrent une volonté affirmée de répondre à la hausse des cas de fraudes. En effet, **au Royaume-Uni, le PSR s'attend à ce que les nouvelles exigences de remboursement poussent indirectement les prestataires financiers à rehausser leurs mesures de prévention et de détection, et chacun sera libre de déterminer comment y parvenir** [5]. C'est sans doute là où **l'approche de l'Australie s'avère plus avantageuse, car l'accord pris entre les institutions financières viendra non seulement assurément bonifier les pratiques de sécurité à travers le secteur, mais aussi les harmoniser**. Ainsi, si plusieurs entités appliquent les mêmes mesures et sont soumises aux mêmes normes, elles risquent d'avoir plus de facilités à partager du renseignement afin de repérer des individus malveillants, et d'identifier des schémas (*patterns*) de transactions frauduleuses interinstitutions.

D'ailleurs, **plusieurs experts sont d'avis que le partage de renseignement constitue un élément clé de la lutte contre la fraude bancaire**, par exemple en anonymisant les transactions [27]. Au-delà de la collaboration interbanques, d'autres professionnels soutiennent **l'importance d'inclure d'autres partenaires tels que les différents fournisseurs de technologie et les fournisseurs de paiements pour privilégier une réponse en amont**, ce qui permettrait d'agir sur différents points d'attaque pour rendre le travail des fraudeurs plus difficile et moins profitable [31]. La *Online Fraud Charter* et le *Online Safety Act* du Royaume-Uni, ainsi que les pourparlers entre le gouvernement australien et le secteur des technologies seraient donc des éléments cruciaux du développement de la stratégie antifraude de ces nations.

Conclusion

Les deux pays tentent de mettre en œuvre des réponses novatrices au fléau de la fraude bancaire en ligne avec leur approche. Bien que l'efficacité des mesures ne pourra être évaluée que dans les prochaines années, on peut penser que **certains éléments de base, communs aux deux approches, constituent des points de départ prometteurs pour toute nation en processus d'élaboration d'une stratégie nationale antifraude**. Notamment, **l'ajustement des mesures de sécurité bancaire semble être au cœur des solutions, non seulement pour responsabiliser les banques, mais aussi pour soutenir la responsabilisation des clients**, par exemple par le biais d'avertissements et systèmes de confirmation de bénéficiaires. En effet, ces pratiques semblent être mises en place pour **inciter les clients à mieux évaluer la légitimité de leurs opérations en temps réel et à renforcer leur diligence lors de transactions risquées**. Finalement, **la collaboration avec les experts, ainsi que les entreprises du secteur des technologies semblent cruciales** pour développer une stratégie efficace et pour assurer une responsabilisation équilibrée de toutes les parties concernées par la fraude.

Tableau comparatif des approches du Royaume-Uni et de l'Australie

	Royaume-Uni		Australie	
	• Obligation de remboursement (responsabilité partagée entre l'institution financière émettrice et réceptrice des transferts frauduleux. • Refus de remboursement autorisé uniquement en cas de négligence grave du client.		• Responsabilisation volontaire des institutions bancaires par l'adoption de diverses mesures antifraude. • Pas de prise de position ferme en matière de responsabilité des institutions financières ou des clients, et aucune directive quant aux mesures de remboursement.	
	Avantages	**Inconvénients**	**Avantages**	**Inconvénients**
Clients	• Recours clairs pour les victimes. • Protection de la clientèle vulnérable.	• Réduction du niveau de diligence requis. • Augmentation des délais pour certains transferts à des fins d'investigation.	• Protections supplémentaires à venir (ex : avertissements et *CoP*)	• Aucun recours clair pour les victimes • Incitation accrue à la diligence
Secteur bancaire	• Incitatif au développement de mesures de sécurité robustes • Incitatif financier à la prévention et détection des fraudes pour éviter le remboursement	• Responsabilité financière accrue. • Manque d'information sur les coûts associés à l'implémentation. • Risque d'entrave aux investissements étrangers et à l'innovation des transferts rapides.	• Harmonisation des pratiques antifraude à travers le secteur bancaire • Concentration des efforts et des investissements vers des solutions préventives	• Aucun incitatif financier à la détection des fraudes (remboursement non obligatoire)

Références

[1] Stripe, (2023, avril) Fraude au paiement push autorisé : De quoi s'agit-il ? *Stripe*.

[2] INTERPOL, (2024, mars). Financial Fraud assessment : A global threat boosted by technology. *INTERPOL*,

[3] Baker, N. (2024, janvier 31). Authorised Push Payment Fraud and the Scam-Safe Accord—Are we doing enough to protect Australians from scammers? *HWL Ebsworth Lawyers*.

[4] Nataraj-Hansen, S. (2024). "More intelligent, less emotive and more greedy": Hierarchies of blame in online fraud. *International Journal of Law, Crime and Justice*, 76, 100652.

[5] Bamber, O. (2024, février 20). The new rules for Authorised Push Payment fraud reimbursement – and what they mean for scam prevention. Lending Standards Board.

[6] Maher, R. (2021). A Critical Analysis of Recent Efforts in the United Kingdom to Tackle Authorised Push Payment Scams and the Impact on the Bank-Customer Relationship. *Trinity College Law Review*, 24, 134-145

[7] Taylor, J. L. et Galica, T. (2020). A New Code to Protect Victims in the UK from Authorised Push Payments Fraud. *Banking and Finance Law Review*. *35*(2), 327-332.

[8] GOV.UK, (2023, juin). Fraud Strategy: Stopping scams and protecting the public, *GOV.UK*.

[9] Chalimont, F. (2021, juillet 9). Cold call et appel à froid : Une prospection efficace ? *Sales & Strategies*.

[10] Decision Telecom. (2023, juin). What are SIM-farms and why companies should not use them. *Decision Telecom*.

[11] Reuters. (2023, juin). UK's payments regulator lays down mandatory reimbursements in APP fraud victims. *Reuters*,

[12] Pay.UK, (2024). How Faster Payments work, Pay.UK.

[13] PSR. (2020, octobre). If card payments are so good, why would I use anything else? *PSR*.

[14] PSR, (2023, décembre). Fighting authorised push payment scams: final decision, *PSR*,

[15] PSR. (2023, décembre). PSR continues to take bold action on APP fraud as it publishes final reimbursement details ahead of 2024 implementation. *PSR*.

[16] PSR. (2023, Août). Authorised push payment scams: The consumer standard of caution, *PSR*.

[17] Financial Services Regulatory Insights. (2023, juin). PSR confirms plans for banks to reimburse APP scam victims.

[18] PSR. (2023, juin). Fighting authorised push payment fraud: A new reimbursement requirement, Response to Septembre 2022 Consultation. *PSR*.

[19] PSR. (2023, juin). Fighting authorised push payment fraud: A new reimbursement requirement; Annex 4: Cost Benefits Analysis. *PSR*.

[20] Financial Conduct Authority. (2021, février). Guidance for firms on the fair treatment of vulnerable customers. *FCA*.

[21] GOV.UK, (2023, novembre). Online Fraud Charter 2023. *GOV.UK*.

[22] Prinsley, A., Yaros, O., Randall, R., Hajda, O., Hepwoth, E. et Maher, A. (2024, mars). The UK Online Safety Regime : Five Months On. *MAYERBROWN*.

[23] GOV.UK. (2024, mai). Online Safety Act: Explainer. *GOV.UK*.

[24] Commonwealth of Australia. (2022). Budget october 2022-23.

[25] Transmit Security, (2024). 6 Initiatives of the 'Scam Safe Accord' & a Ready-Made Solution, *Transmit Security*.

[26] Ministers, (2023, novembre). Government welcomes Scam Safe Accord, *Treasury Ministers*.

[27] PYMNTS. (2024, mars). UK Wants to Turn Faster Payments Into Four-Day Payments. *PYMNTS.Com*.

[28] FitchRatings. (2024). Fraud Reimbursement Costs Are Likely to Rise for UK Banks. *FitchRatings*,

[29] Chaplin, R., Ali, A., Wang, D. et Adams W. (2024) New Rules To Tackle Authorised Push Payment Fraud, *Skadden*,

[30] Sullivan, J. (April 2024). APP fraud : The UK's mandatory reimbursement requirement. *Thomson Reuters Institute*.

[31] PYMNTS. (2023, décembre). What 17 Payments Experts Expect From Instant Payments in 2024 and Beyond. *PYMNTS.Com*.