Plus forts ensemble

Pourquoi la collaboration est-elle le premier pas dans la lutte contre la fraude

Le point de vue d'Interac Corp.

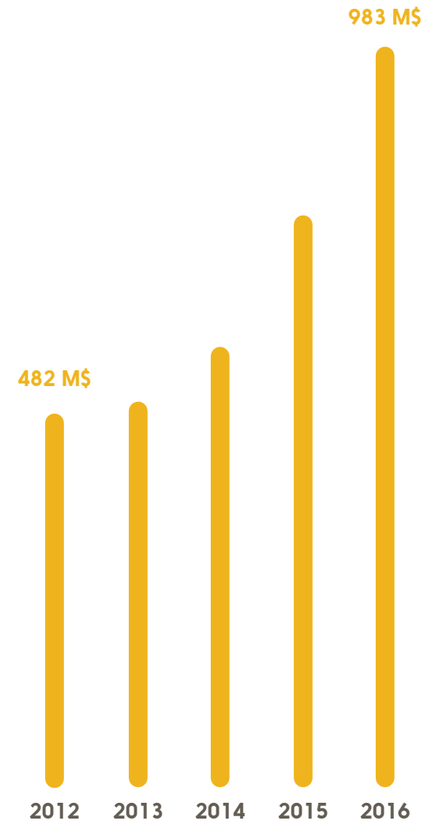
« Nous sommes fermement engagés à nous assurer que les consommateurs puissent avoir accès à leur argent de façon sécuritaire et que les risques de crimes financiers ne soient jamais un frein à l'adoption de nouveaux produits et de nouvelles technologies. »

Introduction

Les deux dernières décennies d'innovations technologiques ont marqué le début d'un monde de connectivité et de commodité sans précédent. Dans le domaine des services financiers, il n'a jamais été aussi facile pour les consommateurs d'accéder à leur argent quand ils le veulent et où ils le veulent, de transférer des fonds à leurs amis ou à des membres de leur famille, de faire des achats en ligne, ou encore, de mettre les gens, les gouvernements et les entreprises en communication.

Toutefois, cette accessibilité et cette facilité d'utilisation sont venues avec un côté plus sombre. Comme cela a été le cas pour toutes les autres innovations du secteur bancaire au cours de l'histoire, des gens mal intentionnés ont utilisé la technologie pour trouver de nouvelles façons de commettre des actes frauduleux. La popularité du commerce électronique, par exemple, a permis d'ouvrir de nouvelles voies à la fraude « sans présence de carte ». Dans ce type de fraude, un criminel utilise des données de carte volées pour se procurer des biens et des services, sans avoir besoin de la carte physique. Au Canada, les pertes totales brutes liées à la fraude dans les comptes de clients canadiens ont dépassé 980 millions de dollars en 2016. Aux États-Unis la même année, les pertes ont totalisé 7,7 milliards de dollars – et on s'attend à ce qu'elles atteignent 12 milliards de dollars d'ici 2020*.

À Interac, nous sommes fermement engagés à nous assurer que les consommateurs puissent avoir accès à leur argent de façon sécuritaire et que les risques de crimes financiers ne soient jamais un frein à l'adoption de nouveaux produits et de nouvelles technologies. La sécurité et l'expérience client sont au cœur de la conception de nos produits. Ainsi, nos efforts portent plus particulièrement sur la prévention de la fraude, alors que nous collaborons étroitement avec nos institutions financières partenaires, les commerçants, les consommateurs et les autorités policières dans un programme continu de réduction du risque visant à établir la confiance. Dans ce livre blanc, nous aborderons les grands axes de ce travail.



Un problème qui prend de l'ampleur

De 2012 à 2016, le montant total brut lié à la fraude au Canada a plus que doublé*. Plus de 95 % de ce montant est attribuable à la fraude par carte de crédit.

* Sources : Statista.com, Association des banquiers canadiens, Interac Corp.

Tout commence par la confiance

La fraude exploite et détruit la confiance, ce qui a une incidence négative importante sur le bon fonctionnement de l'économie.

L'argent, c'est bien connu, est un exercice de confiance à l'échelle de la société qui est maintenu depuis des décennies et des siècles. Un huard ne vaut pas grand-chose en tant que pièce ronde en alliage métallique, mais en tant que pièce de « un dollar », nous savons contre quoi il peut être échangé. La plus grande partie de notre richesse monétaire n'est pas du tout physique; elle se résume plutôt à des entrées dans des registres numériques stockés sur les serveurs des institutions financières. Nous comptons sur nos institutions financières pour nous donner notre argent lorsque nous la demandons et sur les commerçants pour nous remettre nos achats lorsque nous les avons payés. Sans la confiance, nous serions obligés de revenir à une économie d'échange primitive. Je vous échange trois chèvres contre cette brouette.

La fraude, à la base, exploite et détruit la confiance, ce qui a une incidence négative importante sur le bon fonctionnement de l'économie, ainsi que sur les interactions courantes entre les entreprises et les consommateurs. Une institution financière qui fait confiance à un client peut autoriser des transactions dont les montants sont élevés, comme un prêt hypothécaire ou un prêt d'entreprise – une situation dont bénéficient évidemment l'institution financière, le client et l'économie elle-même. Le client se retrouve également dans un cercle vicieux; car si ce dernier fait confiance à son institution financière, il sera beaucoup plus susceptible de profiter des outils qui s'offrent à lui pour aider à prévenir la fraude et à protéger son propre argent – des outils comme la surveillance des transactions, les alertes par courriel et messages texte, le gel du crédit, et ainsi de suite.

C'est dans l'intérêt des institutions financières, des commerçants et de leurs partenaires de collaborer et de partager des renseignements dans le but de renforcer la confiance et d'atténuer les risques de fraude. Même si certains de ces joueurs sont des concurrents sur le marché, les avantages d'une collaboration surpassent largement les risques.

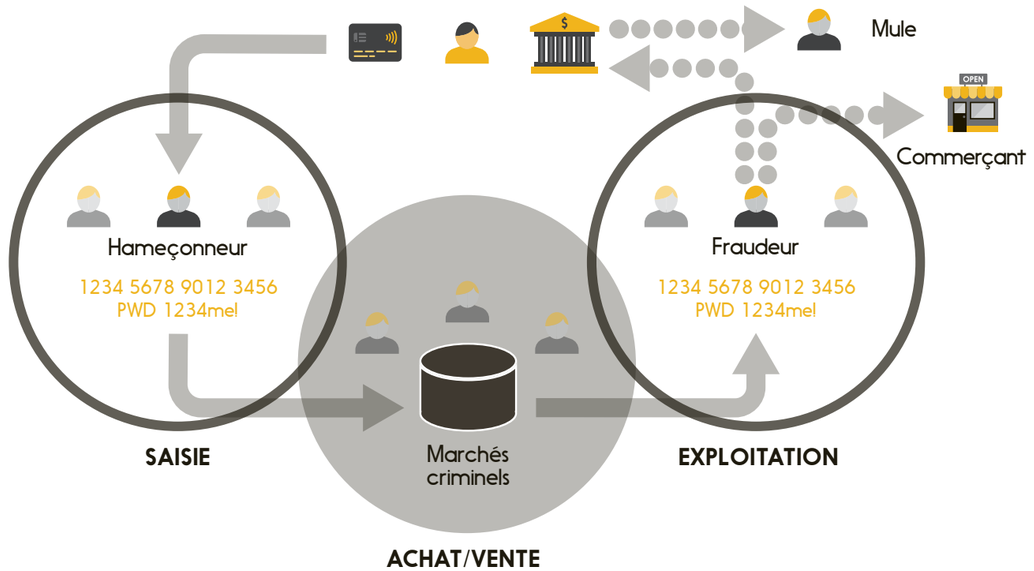
Pourquoi est-il préférable d'agir ensemble au lieu de faire cavalier seul?

Les herbivores se tiennent en groupe pour une raison : s'ils broutent seuls, les prédateurs peuvent les attraper et les dévorer facilement. Et ce n'est pas parce qu'un seul loup, par exemple, est un adversaire plus redoutable qu'un seul caribou. C'est parce que les loups agissent ensemble, et si les caribous ne se regroupent pas – tous les regards tournés vers la limite des arbres, les animaux étant attentifs aux signaux des autres bêtes du troupeau – les loups gagneront.

La technologie qui permet aux consommateurs d'accéder facilement à des biens et à des services est la même technologie qui permet aux criminels de créer facilement des alliances. Le pirate informatique solitaire dans une chambre à coucher – une représentation culturelle encore bien vivante – ne représente plus la menace que nos systèmes financiers doivent affronter. Même si certains loups solitaires exercent toujours leurs activités avec succès, des fraudes sont souvent commises par des réseaux de criminels reliés entre eux numériquement. En général, ces réseaux sont organisés selon les spécialités individuelles des pirates : ceux qui volent des données précieuses et de nature hautement confidentielle, comme les numéros de carte, les noms d'utilisateurs et les mots de passe; ceux qui les vendent sur des marchés noirs; et ceux qui achètent et exploitent ces données pour réaliser des gains financiers, volant souvent de l'argent dans des comptes de clients sans méfiance.

Réseaux clandestins

Les fraudes sont commises par des réseaux de criminels clandestins, qui ont tous leur spécialité; les malfaiteurs n'ont même pas à se rencontrer.



Les malfaiteurs n'ont même pas à se rencontrer : tout comme les marchés en ligne qui mesurent le degré de confiance au moyen de systèmes de réputation, les plateformes criminelles utilisées par les pirates informatiques et les fraudeurs ont leur propre système d'évaluation. En fait, alors que le reste du monde vient à peine de se rendre compte des possibilités d'une « économie collaborative », les criminels ont été parmi les premiers à en tirer parti.

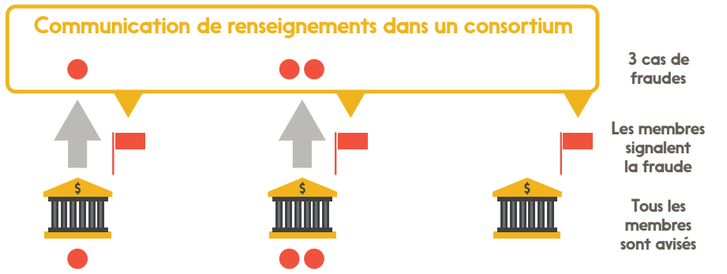
En créant un climat de confiance et en organisant leurs activités virtuellement, les criminels d'aujourd'hui peuvent employer des stratagèmes frauduleux très complexes qui touchent (ou exploitent) de multiples institutions financières et qui ne sont pas limités par des frontières physiques.

Notre réponse à cela doit être tout aussi coordonnée et inflexible. Examinons deux situations hypothétiques.

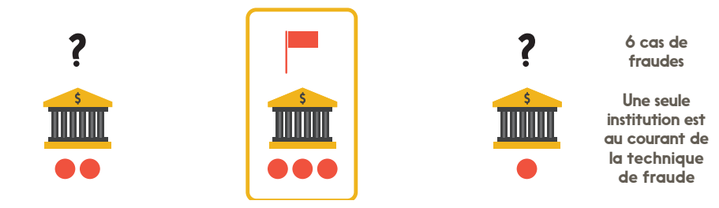
Dans la première, les institutions financières luttent seules contre la fraude et ne communiquent pas de renseignements entre elles. Pour qu'une institution remarque la présence d'un stratagème frauduleux et observe une technique de fraude, ses propres clients doivent avoir été la cible de multiples attaques – ce qui pourrait prendre un certain temps dans le cas d'un stratagème qui cible les clients de nombreuses banques. Dans la deuxième situation, les renseignements pertinents sont communiqués entre les institutions; ainsi, un stratagème frauduleux qui cible seulement quelques clients de plusieurs banques peut être suffisant pour dégager une technique de fraude. De plus, des mesures peuvent être prises beaucoup plus rapidement afin d'empêcher que le stratagème ne se poursuive.

Un homme averti en vaut deux

Dans un consortium qui communique des renseignements sur les activités frauduleuses, non seulement les techniques de fraude sont signalées plus rapidement, mais tous les membres du consortium sont immédiatement avisés – y compris ceux qui n'ont pas encore été victimes de la fraude.



Dans un système en silos, une institution financière doit attendre qu'une tendance se dégage des multiples fraudes perpétrées contre ses propres clients – et comme les autres institutions ne reçoivent pas d'avertissement, elles demeurent vulnérables.



La meilleure protection possède plusieurs niveaux

Notre stratégie de lutte contre la fraude vise à éliminer la fraude au Canada en concentrant nos efforts sur la **prévention** du vol des données requises pour commettre une fraude, sur la **détection** de l'utilisation de ces données et sur notre **réponse** dans les secteurs où le risque est supérieur à la moyenne.

Une véritable efficacité sur les trois fronts exige une variété d'activités. La prévention ne dépend pas seulement de la technologie, elle dépend aussi d'une conception de produit intelligente et elle repose sur l'éducation. La détection est possible grâce à une surveillance continue, à une détection de techniques de fraude et à des alertes en temps opportun. La réponse, pour sa part, est une combinaison de planification, de coordination et d'engagement avec les organismes d'application de la loi.

Ces activités continues nécessitent une attention constante de la part des organisations et la participation active de toutes les composantes de l'écosystème financier et commercial : les institutions financières, les réseaux, les commerçants et les consommateurs.

En tant que réseau axé sur les transactions, nous avons pu jouer un rôle clé dans une approche en consortium visant à lutter contre la fraude. Comme nous relions les institutions financières entre elles – et les relions également aux commerçants et aux clients – nous avons été en mesure d'agir en tant que point central de sensibilisation et de coordination intersystèmes. Les clients des plateformes Débit *Interac*[MD] et Virement *Interac*[MD] ont profité de la surveillance et de l'analyse des transactions et de leurs tendances, ainsi que de leur propre rapport de fraude et d'autres retours d'information qui permettent aux institutions de profiter des premiers signaux d'alerte fournis par leurs pairs. Tout cela est possible non pas grâce à la mise en commun des données de tous les clients, mais grâce au partage d'une quantité de renseignements pertinents suffisante pour permettre la surveillance d'activités suspectes ou anormales et pour que le réseau, les institutions financières et les organismes d'application de la loi déclenchent une enquête et la prise de mesures.

La collaboration est la clé

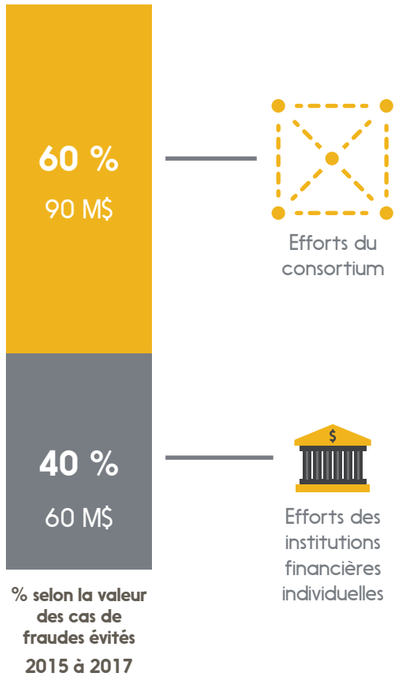
Grâce à la collaboration à l'échelle de l'industrie qui comprend à la fois de nouvelles technologies et le partage de renseignements, la fraude sur le réseau Débit *Interac* a atteint son niveau historique le plus bas.

Cette excellente collaboration a permis à Virement *Interac* d'atteindre l'un des plus bas taux de fraude à l'échelle internationale.

Excellente collaboration = excellents résultats

Grâce aux efforts du consortium, 60 % des cas de fraude ont été évités au cours des trois dernières années (pourcentage mesuré selon la valeur) sur le réseau Virement *Interac*.

Grâce aux efforts des institutions financières, 40 % des cas de fraude ont été évités.



Source : Interac Corp.

Cependant, la communication de renseignements ne suffit pas. La meilleure protection comprend plusieurs niveaux : un dans lequel chaque participant lutte contre la fraude du mieux qu'il peut selon ses propres capacités, et dans lequel les participants soutiennent les efforts des autres afin que le système dans son ensemble soit aussi résilient que possible.

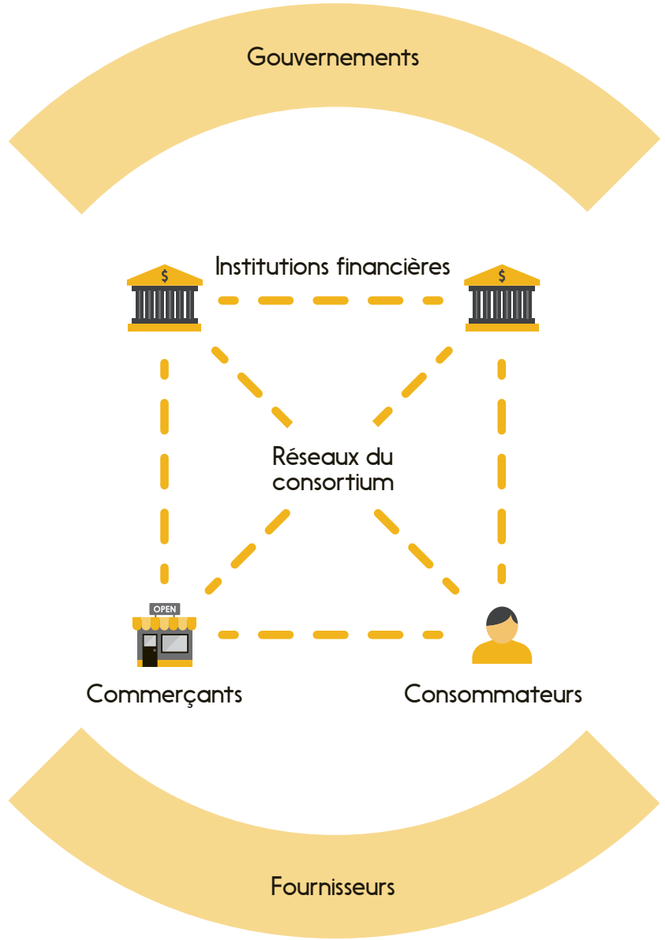
Comme les cartes de débit de marque *Interac* sont utilisées dans des endroits physiques partout au pays pour acheter, par exemple, des biens et des services, nous voulons nous assurer que les commerçants de notre réseau possèdent les outils et les connaissances requises pour détecter et prévenir la fraude aux points de vente. De nos jours, les transactions s'effectuent de plus en plus sur des téléphones intelligents et de nouvelles technologies comme la création de jetons permettent d'extraire le numéro de compte personnel d'un utilisateur en lui attribuant un numéro de compte aléatoire (ou « jeton »). Ce numéro est utile seulement pour la transaction; il est inutile pour les pirates ou les voleurs d'identité. Enfin, nous procurons des technologies sécuritaires aux consommateurs (cartes de débit à puce et à NIP, par exemple) et nous leur donnons des conseils dans le but d'éviter qu'ils soient victimes de fraude – et, par extension, de maximiser le degré de confiance qu'ils accordent à leur institution financière et aux commerçants avec qui ils font affaire.

Dans la même veine, les institutions financières doivent continuer à veiller à ce que leurs propres clients ne soient pas victimes de fraude (ou ne puissent pas commettre de fraude, cela dit) en mettant en œuvre les meilleures pratiques et technologies à leur disposition en matière d'authentification, de surveillance et de rapidité de réponse. Interac permet de multiplier les forces, aidant à améliorer l'efficacité globale des efforts de l'industrie en déployant des mesures à l'échelle du consortium.

Au Canada, le service Virement *Interac* illustre très bien de telles mesures. En effet, grâce à l'excellent esprit de collaboration dont ont fait preuve nos partenaires, nous avons atteint un des plus bas taux de fraude à l'échelle internationale. Bien qu'une seule mesure de sécurité ne soit jamais suffisante pour arrêter complètement la fraude et le vol d'identité, un des meilleurs moyens de se protéger est de tirer parti d'un système composé de multiples collaborateurs; tous indépendants, mais tous connectés.

L'affaire de tous

On peut seulement mettre fin à la fraude si tous les intervenants d'un système financier ou commercial y participent activement : qu'il s'agisse de protéger des données et des renseignements personnels, de détecter les fraudes dès qu'elles surviennent, de partager des renseignements pertinents ou de prendre des mesures rapides et efficaces, nous avons tous plusieurs rôles à jouer.



Une sécurité accrue pour l'avenir

Malgré cette preuve de réussite, nous n'avons certainement pas l'intention de nous reposer sur nos lauriers. La technologie évolue et pratiquement toutes les innovations introduisent de nouveaux moyens d'attaques que les criminels peuvent exploiter. Nous devons continuer à concevoir des produits pour assurer la sécurité, à mettre en place des contrôles adéquats pour détecter les activités frauduleuses lorsque les acteurs malveillants découvrent une faille et nous devons être prêts à apporter une réponse coordonnée et impitoyable.

En tant qu'industrie, nous devons continuer à parfaire nos aptitudes et nos capacités communes sur le plan technique, mais aussi sur les plans organisationnels et collaboratifs afin que les nouvelles attaques nous surprennent seulement la première fois, jamais la deuxième. Ensemble, nous pouvons protéger nos clients et faire en sorte que les réseaux criminels se placent sur la défensive.

Dans nos prochains livres blancs et billets de blogue, nous explorerons plus en profondeur les défis, les initiatives et les réussites qui composent notre lutte collective contre les crimes financiers.

« En tant qu'industrie, nous devons continuer à parfaire nos aptitudes et nos capacités communes sur le plan technique, mais aussi sur les plans organisationnels et collaboratifs. »

Pour en savoir plus sur ce sujet, visitez le site innovation.interac.ca.

Publication : Avril 2018