SERVICE CANADIEN DE RENSEIGNEMENTS CRIMINELS

PRÉVISION NATIONALE DU RENSEIGNEMENT CRIMINEL SUR LES MARCHÉS CRIMINELS CANADIENS : LE BLANCHIMENT D'ARGENT ET LA FRAUDE

2020

DATE DE PUBLICATION : LE 28 SEPTEMBRE 2020

AVANT-PROPOS DU DIRECTEUR GÉNÉRAL DU SERVICE CANADIEN DE RENSEIGNEMENTS CRIMINELS

Je suis heureux de vous présenter la *Prévision nationale du renseignement criminel de 2020 (PNRC) : le blanchiment d'argent et la fraude*. Cette évaluation stratégique donne un aperçu de la portée et de l'ampleur du blanchiment d'argent et d'importants marchés de fraude au Canada ainsi que du rôle du crime organisé dans ces activités criminelles. Elle est fondée sur des données ayant été transmises par des organismes d'application de la loi à l'échelon fédéral, provincial ou municipal, de l'information tirée de sources ouvertes et des renseignements fournis par d'autres organismes gouvernementaux, du Canada et d'ailleurs, au sujet des menaces de longue date comme des menaces nouvelles qui pèsent sur le Canada.

Bien que la plupart des renseignements produits par le SCRC ne soient partagés qu'avec les organismes d'application de la loi, le SCRC diffuse de plus en plus de renseignements au public afin de le sensibiliser à la nature et à l'étendue des menaces du crime organisé au Canada. Une telle perspective nationale nous aide à nous assurer que la communauté chargée de l'application de la loi, le gouvernement et le grand public canadien ont la même vision des crimes graves et du crime organisé. Elle favorise également la création et l'entretien de partenariats essentiels à notre lutte contre cette menace.

Le SCRC collabore activement avec ses bureaux provinciaux et de nombreux organismes d'application de la loi fédéraux, provinciaux et municipaux. Nous échangeons avec nos partenaires de l'information essentielle pour évaluer et combattre les menaces associées au crime organisé. Je tiens à remercier sincèrement nos partenaires pour leur apport précieux à l'élaboration du présent rapport.

Rob Gilchrist, surintendant principal
Directeur général
Service canadien de renseignements criminels

TABLE DES MATIÈRES

SOMMAIRE

Répercussions du marché

Estimation de l'argent blanchi au Canada : *de 45 à 113 milliards de dollars canadiens*

Certains blanchisseurs d'argent professionnels blanchissent *des centaines de millions de dollars canadiens par année*

Pertes dues à la fraude signalées au Centre antifraude du Canada (CAFC) en 2019 : *100 M$CAN*

Parmi les *victimes* :

- ✓ Individus (économies de vie)
- ✓ Gouvernement (revenus, services sociaux, réputation)

Perception : criminalité en col blanc
Réalité : groupes du crime organisé (GCO) interreliés au Canada et à l'étranger

Facilitateurs de la criminalité

Le placement de propriété légale dans des sociétés, des fiducies, des partenariats ou des prête-noms permet de *cacher la véritable propriété* des actifs

La *législation* n'exige pas que les courtiers en hypothèques, les prêteurs privés, les avocats et les notaires (au Québec) signalent à CANAFE les activités suspectes ou les transactions en espèces importantes

Connectivité mondiale

- ✓ Plateformes internationales en ligne pour faciliter la fraude et le blanchiment d'argent
- ✓ Accès quasi instantané à des victimes dans le monde entier

Sources de données

- ✓ Plateformes non protégées en ligne (noms, DDN, adresses et photos)
- ✓ Vol de données dans les systèmes du gouvernement ou des institutions financières
- ✓ Des courtiers en données vendent des listes de contacts ciblées
- ✓ Achat, vente et échange de données financières et de guides dans le Web caché

Protection offerte par des intermédiaires comme des sociétés du secteur privé, des GCO de plus bas échelon et des mules

Défis pour la police

Besoin de formation, ressources et connaissances accrues pour les organismes d'application de la loi en relation au blanchiment d'argent

La complexité des ententes commerciales internationales rend le blanchiment d'argent fondé sur les transactions commerciales (BATC) difficile à reconnaître

L'anonymat en ligne (difficile de déterminer la base des activités et de désigner les organismes compétents)

La lutte contre les activités *multi-juridictionnelles* nécessite des partenariats avec des agences au Canada et à l'étranger

Le blanchiment d'argent et la fraude seraient *sous-déclarés*

Blanchiment d'argent

La majorité des GCO cherchent à *camoufler les produits de leurs crimes*

176 GCO évalués en 2019 trempent dans le blanchiment d'argent, mais il y en aurait plus

76 p. 100 de ces GCO sont basés *en Ontario, en Colombie-Britannique et au Québec*

50 p. 100 entretiennent des liens à l'étranger

- ✓ Cinq principaux pays : États-Unis, Mexique, Chine, Colombie et Australie
- ✓ Près de la moitié de ces groupes trempent dans le marché de la cocaïne

Blanchiment fondé sur les transactions commerciales

Sert à déplacer *des centaines de millions de dollars* en passant par le Canada

Des *blanchisseurs professionnels* canadiens font d'importantes transactions de BATC de clients de l'étranger

Les paiements versés par des *sociétés d'import-export tierces et indépendantes* dans des territoires propices au BATC représentent un risque important

Cryptomonnaie

Souvent utilisée pour *payer des fraudeurs*, faire des achats sur le *Web caché* et blanchir de l'argent

Le recours aux services et outils d'anonymat pour brouiller l'origine des transactions *a triplé* en un an

Fraudes les plus souvent signalées

Les escroqueries concernant les services gouvernementaux minent la confiance du public envers le gouvernement

12 GCO font du *vol d'identité*

Harponnage :
pertes de 21,4 M$CAN +

Stratagèmes de rencontre :
pertes de 24 M$CAN +

3200 incidents de *logiciels de rançon* par jour ;
pertes moyennes : de 1 à 3 M$CAN par incident

Stratagèmes ciblant les aînés : pertes de 35 M$CAN +

9 GCO impliqués dans des stratagèmes de *fraude en valeurs mobilières* pouvant entraîner des pertes de plusieurs millions de dollars

22 GCO impliqués dans la *fraude par carte de paiement*, dont les pertes sont rarement déclarées

8 GCO impliqués dans la *fraude immobilière*

INTRODUCTION

Contexte

La PNRC de 2020 sur le blanchiment d'argent et la fraude est produite par le Bureau central du SCRC, en collaboration avec ses dix bureaux provinciaux qui suivent le processus d'évaluation intégrée des menaces (EIM), ses organismes membres et d'autres partenaires à l'échelon fédéral et provincial. La PNRC est l'un des principaux produits du SCRC pour répondre au besoin des dirigeants de la communauté de l'application de la loi, des décideurs du gouvernement et du grand public canadien de disposer de renseignements stratégiques sur la portée et l'ampleur des marchés criminels au Canada.

Structure

La présente PNRC représente une évaluation stratégique approfondie de la menace que font peser sur le Canada le blanchiment d'argent et la fraude à l'intérieur des frontières du pays et à l'échelle internationale. Une attention particulière est accordée aux préoccupations croissantes liées au blanchiment d'argent au Canada et à d'importants aspects du blanchiment d'argent, notamment le blanchiment d'argent fondé sur les transactions commerciales (BATC) et la cryptomonnaie. Le rapport porte également sur différentes formes de fraude qui représentent des menaces importantes pour le Canada, y compris la fraude en marketing de masse, la fraude en valeurs mobilières, la fraude par cartes de paiement et la fraude immobilière.

Répercussions du blanchiment d'argent

Le blanchiment d'argent permet aux criminels d'introduire les produits de leurs activités criminelles dans l'économie légale du Canada, d'en camoufler la provenance et d'éviter la détection et la confiscation de biens ou de fonds obtenus illégalement. L'Office des Nations Unies contre la drogue et le crime (ONUDC) estime que le montant d'argent blanchi à l'échelle mondiale se situe entre deux et cinq pour cent du produit intérieur brut (PIB) mondial. Si on applique cette formule aux données actuelles qui concernent le Canada[1], la somme de l'argent blanchi au Canada atteindrait entre 45 et 113 milliards de dollars canadiens.

Les professionnels qui font du blanchiment d'argent (PBA), aussi appelés des fournisseurs de services de blanchiment d'argent, sont particulièrement préoccupants, puisqu'ils coordonnent les opérations pour des groupes du crime organisé (GCO), des individus criminalisés et pour eux-mêmes. Les PBA vendent leurs services aux GCO et aux autre criminels, mais ne font souvent pas partie des activités criminelles qui génèrent le produit du crime qu'ils blanchissent. Cela leur permet de rester à l'abri des infractions sous-jacentes et rend difficile pour les enquêteurs et les procureurs de prouver la connaissance de l'origine illicite des fonds. Certains PBA au Canada blanchiraient des centaines de millions de dollars canadiens chaque année.

Outre le recours à de tels intermédiaires, le blanchiment d'argent au Canada est rendu possible par sa nature clandestine inhérente, une législation qui n'exige pas une transparence totale et la complexité des enquêtes sur les stratagèmes de BATC.

[1] Le PIB du Canada en 2018 était estimé à 1,7 billion de dollars américains ou 2,26 billions de dollars canadiens, selon un taux de change de 1,33 $CAN pour un dollar américain.

Répercussions du marché de la fraude

Chaque année, la fraude fait perdre des millions de dollars aux Canadiens. En 2019, les pertes déclarées au Centre antifraude du Canada (CAFC) s'élevaient à près de 100 millions de dollars canadiens. La fraude prive des particuliers de leurs économies, entraîne des pertes fiscales et peut accentuer la pression financière qui pèse sur les services sociaux financés par le gouvernement. Outre l'aspect monétaire, certains stratagèmes de fraude visent aussi à obtenir des données personnelles pour faciliter d'autres crimes, comme le vol d'identité. Par ailleurs, de nombreuses victimes ressentent, à tort, un sentiment de honte qui peut mener à des problèmes de santé mentale, à la consommation abusive de substances intoxicantes, à l'isolement et au suicide.

Même si elles ont accès à beaucoup d'information sur les stratagèmes de fraude, les victimes ne prennent souvent pas le temps de se demander si elles pourraient être la cible d'un fraudeur, que ce soit à cause de la pression exercée par les criminels, de l'isolement social, du manque de connaissances sur le plan financier ou d'un excès de confiance.

La criminalité financière, aussi appelée criminalité en col blanc, est commise par des criminels ayant une importante capacité et par des GCO interreliés, au Canada et à l'étranger. Tandis que certains GCO canadiens exploitent directement des entreprises de vente sous pression (télémarketing frauduleux), d'autres récolteraient simplement une partie des profits. Les profits réalisés, qui sont substantiels, servent souvent à financer d'autres activités criminelles, principalement l'importation et le trafic de drogue.

Les GCO et les criminels qui continuent de faire de la fraude en personne risquent davantage de se faire prendre, mais de nombreux autres utilisent de nouveaux outils, technologiques ou autres. Cette tendance pose des défis en constante évolution pour les organismes d'application de la loi.

FACILITATEURS DE LA CRIMINALITÉ ET DÉFIS POUR LA POLICE

La section qui suit porte sur les facilitateurs clés liés au blanchiment d'argent, au BATC et à la cryptomonnaie, ainsi que ceux qui servent aux criminels dans la plupart des marchés de la fraude. En fait, les termes « facilitateur de la criminalité » et « défi pour la police » sont souvent interchangeables – ils offrent simplement un point de vue différent. Les deux points de vue sont traités ci-dessous.

Facilitateurs de la criminalité : blanchiment d'argent (incluant celui fondé sur les transactions commerciales)

Nature clandestine

Le blanchiment d'argent, qui est une activité clandestine, est souvent dissocié de l'infraction sous-jacente qui a généré les fonds illicites. Les GCO et autres criminels peuvent donc mener leurs activités sans s'exposer à un risque élevé d'être détectés par les organismes d'application de la loi.

Propriété effective

La propriété effective est un terme utilisé pour représenter l'individu qui gère un bien ou une opération ou qui en tire profit au bout du compte. Les criminels cachent l'identité des véritables propriétaires de biens aux organismes d'application de la loi et de réglementation afin de ne pas éveiller les soupçons et de réduire le risque de saisie. Le manque de transparence liée à la propriété effective facilite la dissimulation de l'identité des véritables propriétaires de biens de toutes sortes, y compris les entreprises, les biens immobiliers, les biens personnels, les comptes bancaires et les investissements, en accordant la propriété légale à des sociétés, des fiducies, des partenariats ou des prête-noms.

Actuellement, le gouvernement fédéral et plusieurs gouvernements provinciaux tentent de corriger les lacunes associées à la propriété effective en adoptant des règlements visant la transparence en vue d'éviter le recours à des sociétés et à des partenariats à des fins criminelles, dont le blanchiment d'argent (voir le **tableau 1**). Ces nouvelles exigences pourraient aider les organismes d'application de la loi à identifier les véritables propriétaires des biens dans le cadre des enquêtes sur le blanchiment d'argent.

Tableau 1 – Nouvelles réglementations

Loi canadienne sur les sociétés par actions Depuis juin 2019, toutes les sociétés constituées en vertu d'une loi fédérale doivent tenir un registre, accessible aux organisations d'application de la loi, aux autorités fiscales et à certains organismes de réglementation, des personnes qui ont un contrôle important sur une entreprise. Au niveau provincial, la Colombie-Britannique, la Saskatchewan, le Manitoba et le Québec ont adopté des règlements similaires concernant les sociétés constituées en société provinciales, qui en sont à divers stades de mise en œuvre.
Land Owner Transparency Act (LOTA) de la C.-B. La LOTA, qui a reçu la sanction royale en 2019 et n'est pas encore entrée en vigueur, exigera la divulgation de toutes les structures individuelles, corporatives et de partenariat qui ont directement ou indirectement un intérêt bénéficiaire dans une propriété en Colombie-Britannique, ainsi que la création d'un registre public consultable de ces informations. La Colombie-Britannique sera la première province à aborder la question de la propriété véritable dans l'immobilier.

Lacunes dans les obligations de signalement de la LRPCFAT

Les professionnels qui participent aux transactions immobilières n'ont pas tous des obligations en vertu de la *Loi sur le recyclage des produits de la criminalité et le financement des activités terroristes* (LRPCFAT). Comme les courtiers hypothécaires, les prêteurs privés, les avocats et les notaires (au Québec) ne sont pas visés par la LRPCFAT, ils ne sont pas tenus de signaler les activités douteuses ou les transactions importantes au comptant au CANAFE. Ceci permet aux criminels et à des professionnels complices d'exploiter ces personnes pour blanchir des fonds et camoufler leurs activités.

Défis pour la police : blanchiment d'argent (incluant celui fondé sur les transactions commerciales)

Un besoin de formation et de ressources accrues

Un besoin pour une formation, des ressources et des connaissances accrues sont les défis les plus souvent identifiés par la communauté d'application de la loi en matière de blanchiment d'argent – des lacunes qui devront être comblées afin de garantir une image plus précise de la menace et d'élaborer une réponse plus ciblée à la menace.

Complexité des ententes commerciales internationales

Étant donné que les activités de blanchiment d'argent se cachent dans la vaste portée de l'économie et des systèmes financiers légitimes du Canada, les autorités chargées de l'application de la loi doivent non seulement détecter les stratagèmes de blanchiment d'argent, mais aussi les relier à la criminalité.

Le BATC est difficile à détecter, compte tenu de la complexité du commerce international, de la facilité avec laquelle les produits de la criminalité peuvent être mélangés à des fonds légitimes, de l'absence de réglementation ou de surveillance des accords entre entreprises internationales et du volume de produits importés et exportés qui traversent la frontière. Les PBA qui ont recours au BATC peuvent participer aux volets de l'importation et de l'exportation. Cette méthode de blanchiment d'argent exige la complicité des deux parties, mais les stratagèmes sont simplifiés lorsque les blanchisseurs contrôlent à la fois la société qui expédie (ou qui prétend expédier) des biens dans un autre pays et les sociétés à l'étranger qui reçoivent ces biens.

Facilitateurs de la criminalité : marchés de la fraude

Connectivité mondiale

La connectivité mondiale, rendue possible par Internet, les appareils intelligents et les médias sociaux, permet aux criminels d'étendre la portée de leurs activités. De plus en plus de stratagèmes de fraude ont une portée internationale, et le recours à la technologie pour faciliter ces crimes permet d'avoir un accès quasi instantané à des victimes dans le monde entier.

Le caractère illimité des plateformes en ligne ainsi que l'évolution constante des technologies mobiles et sans fil procurent aux criminels de plus en plus de possibilités de cibler des utilisateurs par l'intermédiaire de leurs appareils mobiles, dans une relative impunité. L'utilisation grandissante du Web et des technologies numériques, les failles de sécurité et l'élaboration croissante d'attaques complexes qui reposent précisément sur ces failles exposent les gens, les institutions et les gouvernements à des menaces à la cybersécurité.

Sources de données

De plus en plus de données personnelles et financières sont facilement accessibles aux criminels. En plus de la traditionnelle fouille de poubelles pour récupérer des documents papier qui auraient été jetés au rebut de façon inappropriée (par exemple, des états financiers et des dossiers médicaux jetés à la poubelle au lieu d'être déchiquetés ou incinérés), les criminels peuvent passer différentes plateformes Web au peigne fin pour obtenir des renseignements sensibles comme des noms, des dates de naissance, des adresses et des photos. Le forage de données facilite des activités criminelles comme l'hameçonnage (par lequel les criminels communiquent avec des individus tout en prétendant appartenir à des entités réputées afin de provoquer la divulgation d'informations personnelles), l'extorsion et le vol d'identité.

Pour faciliter leurs activités frauduleuses de marketing ciblé, les criminels peuvent mettre la main sur des données personnelles en accédant illégalement à des systèmes à accès restreint (par exemple, en utilisant un maliciel pour

infiltrer les systèmes du gouvernement ou des institutions financières afin d'avoir accès aux dossiers) et avoir recours aux services de courtiers en données, c'est-à-dire des entreprises qui tirent des données personnelles de différentes sources (médias sociaux, revues, organismes de bienfaisance, concours, programmes de fidélité, etc.) puis qui les vendent à d'autres entreprises pour les fins du marketing. Ces courtiers peuvent fournir les coordonnées de certains groupes de personnes en fonction de différents critères démographiques, comme l'âge, le lieu de résidence et les centres d'intérêt.

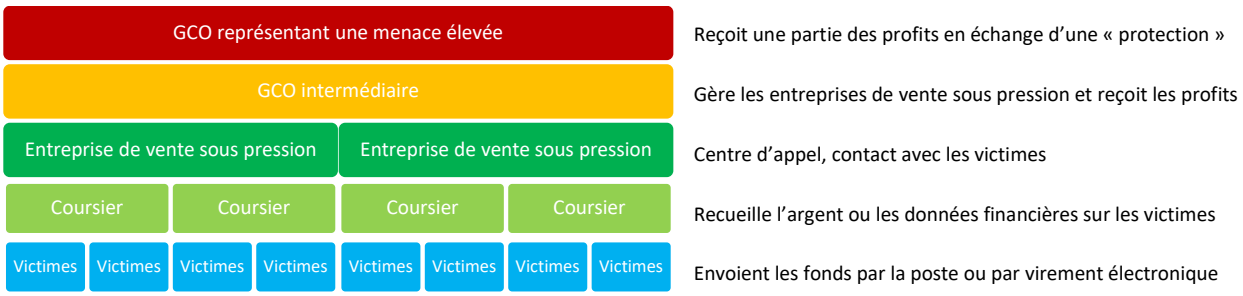
Le Web profond est de plus en plus intéressant pour l'achat, la vente et le transfert, dans l'anonymat, de données financières et de marches à suivre pour mener à bien des stratagèmes de fraude. La société de cybersécurité Sixgill, dans son rapport sur la fraude financière clandestine de 2019, indique que les données associées à plus de 23 millions de cartes de crédit et de débit étaient disponibles dans le Web profond pendant la première moitié de l'année 2019. De plus, les fraudeurs amateurs peuvent trouver dans le Web profond des guides pour se lancer dans la criminalité financière : la société de renseignement Terbium Labs a publié en 2019 un rapport qui portait sur quelque 30 000 guides sur la fraude qui se trouvaient dans le Web profond.

Protection

Différents intermédiaires, notamment des sociétés de promotion, peuvent être exploités pour leur vaste réseau de contacts acquis par l'entremise de courriels, de sites Web, de forums et d'inscriptions à des publipostages. Ainsi, les victimes ne peuvent pas remonter jusqu'à eux.

Les fraudeurs sont aussi protégés par la compartimentalisation des stratagèmes de fraude (voir la **figure 1**). Différents GCO et individus peuvent réaliser les étapes des stratagèmes, ce qui empêche les organismes d'application de la loi de remonter jusqu'aux groupes représentant une menace plus élevée et fait augmenter le niveau de difficulté des enquêtes. Des fonds sont transférés par l'entremise d'entreprises de transfert de fonds (ETF), et ce sont les coursiers qui entrent en contact avec les victimes, au besoin. Un exemple de ce dernier sont des individus qui sont parfois recrutés par le biais d'offres d'emploi frauduleuses dans lesquelles on leur fait croire qu'ils traiteront des paiements pour une entreprise dans le confort de leur foyer alors qu'en fait, ils protégeront des criminels en empêchant les victimes d'y avoir directement accès. Pour réaliser des stratagèmes du genre, il faut souvent des listes de contacts, une personne qui produit de fausses lettres et de faux chèques (pour l'escroquerie du prix gagné), une imprimante pour imprimer ces documents et un fournisseur de services postaux. Dans certains cas, les fournisseurs de services ne savent pas qu'ils participent à une activité criminelle.

Figure 1 – Exemple de compartimentalisation



Défis pour la police : marchés de la fraude

Anonymat

Le Web est une plateforme virtuelle qui permet aux criminels de sévir dans l'anonymat, ce qui complique la tâche des membres de la communauté de l'application de la loi qui veulent cibler les fraudeurs au pays et à l'étranger. En outre, il est difficile de déterminer la base des activités criminelles et le principal organisme d'application de la loi responsable, ce qui nuit à certaines enquêtes.

Plusieurs territoires de compétence touchés

De plus en plus de stratagèmes frauduleux touchent plusieurs territoires de compétence, voire plusieurs pays. Par conséquent, les enquêtes sont complexes, nécessitent beaucoup de ressources et exigent parfois la collaboration de plusieurs organismes d'application de la loi à l'intérieur comme à l'extérieur du Canada. Cette collaboration peut parfois être difficile lorsqu'il s'agit de travailler avec certains pays qui se montrent moins coopératifs.

Signalements limités

Un grand nombre de fraudes, toutes catégories confondues, ne seraient pas signalées, probablement car les victimes ont honte, craignent des représailles ou ne savent pas à qui s'adresser.

Il n'existe pas de statistiques exhaustives sur les plaintes déposées dans l'ensemble du Canada, parce que les victimes qui signalent les fraudes s'adressent à différentes organisations, notamment le CAFC[2], les commissions provinciales des valeurs mobilières, les banques, les tribunaux civils et différents services de police. De plus, les tierces entreprises sont souvent réticentes à donner de l'information sur la fraude par crainte de ternir leur réputation et de perdre des clients.

Sans statistiques exhaustives sur le nombre de plaintes déposées, le nombre de victimes et le coût des stratagèmes de fraude, il est difficile d'évaluer l'incidence globale de la fraude sur la société canadienne ainsi que la mesure dans laquelle la menace associée à différentes formes de fraude évolue.

[2] Néanmoins, malgré l'absence de rapports unifiés, les données du CAFC fournissent l'aperçu le plus complet disponible de ce qui se passe au Canada.

BLANCHIMENT D'ARGENT

Faits saillants

- La majorité des GCO et des criminels cherchent à dissimuler l'origine des produits de leurs crimes. En 2019, 176 GCO évalués seraient impliqués dans le blanchiment d'argent, mais le nombre réel de groupes impliqués serait en fait plus élevé.
- Environ la moitié des 176 GCO canadiens impliqués dans le blanchiment d'argent entretiennent des liens à l'étranger, surtout aux États-Unis, au Mexique, en Chine, en Colombie et en Australie. Près de la moitié des groupes qui entretiennent des liens à l'étranger sont aussi impliqués dans le marché de la cocaïne.
- C'est en Ontario qu'on a signalé le plus grand nombre de groupes impliqués dans le blanchiment d'argent, la Colombie-Britannique et le Québec se classant aux deuxième et troisième rangs. Ensemble, ces trois provinces regroupent plus de 76 p. 100 de tous les groupes qui se livrent à cette activité au Canada.
- Au cours des deux dernières années, le gouvernement fédéral et certains gouvernements provinciaux ont adopté des modifications législatives en vue de renforcer la réglementation visant à lutter contre le blanchiment d'argent, y compris l'actualisation des exigences d'enregistrement de la propriété effective et la modification de l'infraction du blanchiment d'argent dans le *Code criminel* afin d'améliorer le taux de réussite des mises en accusation. Malgré ces modifications, d'autres questions législatives continuent de nuire aux interventions du Canada pour la répression du blanchiment d'argent.

Introduction

Dans son évaluation la plus récente de la situation au Canada, en 2016, le Groupe d'action financière international (GAFI) a signalé que même si le Canada dispose d'une réglementation solide pour lutter contre le blanchiment d'argent, il manque certains éléments dans le cadre législatif et la mise en application des dispositions législatives. Dans son rapport, le GAFI signale aussi que les résultats de la répression ne sont pas proportionnels aux risques de blanchiment d'argent au pays. En novembre 2018, dans le cadre d'un examen de la LRPCFAT, le Comité permanent des finances de la Chambre des communes a entendu des témoins déclarer que le « blanchiment à la neige » et le « modèle de Vancouver » étaient associés au Canada et endommageaient la réputation du pays dans sa lutte contre le blanchiment d'argent.

Le rapport annuel de 2018-2019 du Centre d'analyse des opérations et déclarations financières du Canada (CANAFE) faisait état de plus de 2200 divulgations aux organismes d'application de la loi du Canada et à des groupes étrangers de renseignements financiers. Plus de 70 p. 100 des divulgations étaient liées à des activités présumées de blanchiment d'argent, les trois principales infractions sous-jacentes étant la fraude (32 p. 100), la drogue (30 p. 100) et la fraude fiscale (11 p. 100).

Des organismes et des institutions partout dans le monde décrivent le blanchiment d'argent comme un processus à trois étapes : le placement, la dispersion et l'intégration. Selon la complexité du stratagème, les trois étapes ne sont pas toutes nécessaires pour blanchir les produits de la criminalité. D'après le modèle du CANAFE, la première étape est le placement des produits de la criminalité dans le système financier. La deuxième étape consiste à dissimuler davantage l'origine des fonds en ajoutant des opérations financières de façon à compliquer la vérification de l'acheminement, de la source ou de la propriété des fonds illégaux. La dernière étape vise à intégrer les produits de la criminalité recyclés dans l'économie par des moyens légitimes. La **figure 2** à la prochaine page illustre les trois étapes du processus de blanchiment d'argent.

Analyse du marché

Des membres de GCO et autres criminels se livrent au blanchiment d'argent, des niveaux les plus élémentaires aux régimes plus complexes qui superposent et déguisent la source de financement. Ils utilisent des fonds illicites pour payer des biens immobiliers, pour acheter des articles de luxe, comme des véhicules, et ont recours à des entreprises du secteur privé pour camoufler la véritable provenance de ces fonds. Les GCO qui réalisent des profits limités qu'ils réussissent à

camoufler grâce à des techniques de blanchiment de base n'ont pas besoin d'utiliser des stratagèmes plus complexes. En revanche, les GCO qui accumulent beaucoup d'argent au moyen de leurs activités criminelles adoptent souvent des méthodes avancées, ainsi que les techniques plus simples, pour blanchir les fonds qu'ils ont obtenus illégalement.

Figure 2 – Les trois étapes du processus de blanchiment d'argent, développé par le CANAFE

Implication des criminels et portée des activités au pays

De 2015 à 2019, 25 p. 100 des GCO en moyenne étaient impliqués dans le blanchiment d'argent au Canada. Actuellement, 176 des 680[3] GCO évalués se livreraient à cette activité. Étant donné que la majorité des criminels qui obtiennent des fonds illégalement cherchent à camoufler l'origine des produits de leurs activités, le nombre réel de groupes qui se livrent au blanchiment d'argent serait supérieur à 176.

C'est en Ontario qu'on a signalé le plus grand nombre de groupes impliqués dans cette activité, la Colombie-Britannique et le Québec se classant aux deuxième et troisième rangs. Ensemble, ces trois provinces regroupent plus de 76 p. 100 de tous les groupes impliqués recensés à l'échelle nationale (voir la **figure 3**).

Comme l'illustre la **figure 4**, les groupes criminels qui se livrent au blanchiment d'argent sont aussi impliqués dans d'autres marchés, principalement deux marchés de drogue importants : 115 groupes impliqués dans le blanchiment d'argent (65 p. 100) sont aussi impliqués dans le marché de la cocaïne, 45 groupes (25 p. 100) sont impliqués dans le marché de la méthamphétamine et 43 groupes (près de 25 p. 100), dans les marchés de la cocaïne et de la méthamphétamine.

Les GCO impliqués dans le blanchiment d'argent et dans les marchés de la cocaïne et de la méthamphétamine se trouvent dans l'ouest du Canada, dans les provinces des Prairies, en Ontario, au Québec et au Nouveau-Brunswick. Parmi ces GCO, il y a notamment des chapitres de bandes de motards hors-la-loi (BMHL) et plusieurs PBA. Les activités liées au blanchiment d'argent des groupes impliqués dans l'importation et la distribution de drogue sous-entendent l'envoi de fonds ou le règlement de dettes par l'entremise de systèmes d'autres transferts de valeur (tels que l'échange ou le commerce de biens ou d'autres actifs) vers les pays d'où proviennent les drogues illicites et les précurseurs chimiques.

Figure 3 – Proportion des GCO impliqués dans le blanchiment d'argent en 2019, par province

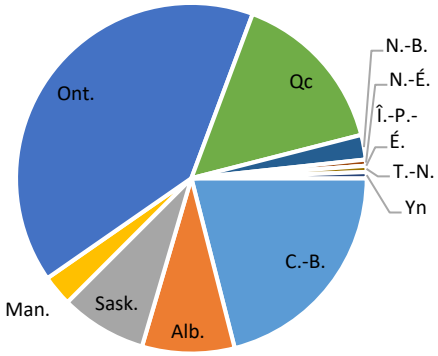
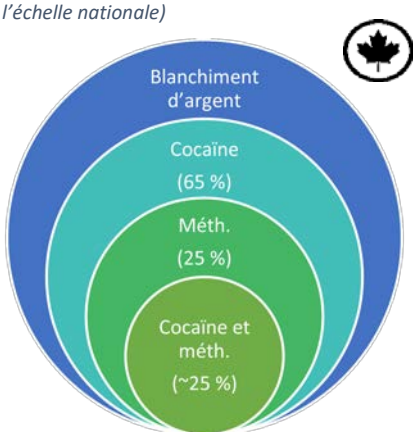


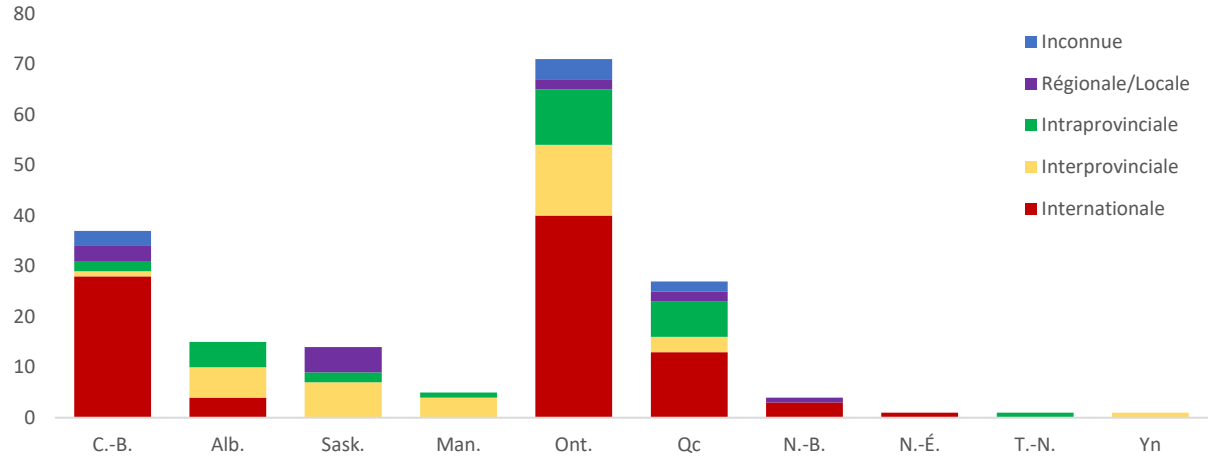
Figure 4 – Autres marchés dans lesquels sévissent les GCO impliqués dans le blanchiment d'argent (à l'échelle nationale)



[3] Il y a 1200 GCO supplémentaires qui ne sont pas évalués dans le processus d'EIM à présent, étant donné l'absence d'informations récentes et significatives qui entrave une évaluation précise et complète de leurs activités criminelles.

Environ 37 p. 100 des groupes impliqués dans le blanchiment d'argent entretiennent des liens intraprovinciaux et interprovinciaux (voir la **figure 5**) et exercent leurs activités à divers endroits au Canada, ce qui signifie que les produits de leurs activités criminelles touchent les territoires de compétence de plusieurs services de police. Parmi ces groupes, il y a des membres de chapitres de BMHL de l'Ontario et du Québec, ainsi que des membres de groupes criminels à la structure de la mafia. Des gangs de rue qui entretiennent des liens interprovinciaux seraient également impliqués dans le blanchiment d'argent.

Figure 5 – Nombre de GCO impliqués dans le blanchiment d'argent par province, selon la portée géographique de leurs activités*



**Aucun groupe évalué de l'Île-du-Prince-Édouard ne serait impliqué dans le blanchiment d'argent.*

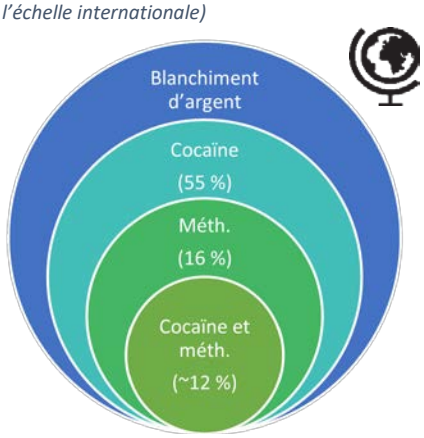
Implication de criminels et portée des activités à l'étranger

Environ 50 p. 100 (89) des 176 GCO évalués entretiennent des liens à l'étranger, surtout aux États-Unis, au Mexique, en Chine, en Colombie et en Australie. Étant donné que certains groupes sont aussi associés aux marchés de la cocaïne et de la méthamphétamine, il n'est pas surprenant de voir certains pays sources de drogue parmi ceux où les GCO impliqués dans le blanchiment d'argent entretiennent le plus de liens.

Selon le CANAFE, les fournisseurs de services de blanchiment d'argent (aussi appelés PBA) basés au Canada ont des liens clés avec l'Asie, le Moyen-Orient et l'Amérique latine. Ces fournisseurs de services agiraient pour le compte de GCO transnationaux et feraient des opérations financières légitimes ou frauduleuses ou mélangeraient des fonds obtenus illégalement à des paiements légitimes. De plus, on soupçonne des blanchisseurs d'argent d'avoir recours à des ETF et des systèmes informels de transfert de fonds (SITF) pour la collecte d'argent et les stratagèmes qui impliquent le transfert d'argent de l'Asie et du Moyen-Orient vers le Canada.

Comme les groupes qui exercent leurs activités au pays, les groupes qui entretiennent des liens à l'étranger sont aussi impliqués dans deux marchés importants de la drogue (voir la **figure 6**) : 49 groupes (55 p. 100) impliqués dans le blanchiment d'argent sont aussi impliqués dans le marché de la cocaïne, 14 groupes (16 p. 100) sont impliqués dans le marché de la méthamphétamine et 12 groupes (près de 13 p. 100), dans les marchés de la cocaïne et de la méthamphétamine.

Figure 6 – Autres marchés dans lesquels sévissent les GCO impliqués dans le blanchiment d'argent (à l'échelle internationale)



Professionnels qui font du blanchiment d'argent

Les GCO et les criminels qui blanchissent des fonds en ayant recours à des professionnels qui offrent leurs services moyennant des frais représentent un intérêt particulier pour les organismes d'application de la loi. Les PBA coordonnent des opérations pour des GCO, des criminels et eux-mêmes. Ils peuvent être des professionnels comme

des comptables, des banquiers ou des avocats corrompus ou malhonnêtes ou encore des propriétaires ou affiliés d'ETF ou de sociétés commerciales (import-export). Ces PBA vendent leurs services à des GCO et d'autres criminels, mais participent rarement aux activités criminelles qui ont généré les produits de la criminalité qu'ils blanchissent. Cette façon de faire leur permet de se dissocier de l'infraction sous-jacente et complique la tâche des enquêteurs et des procureurs qui doivent prouver que le blanchisseur connaît l'origine illicite des fonds. Certains PBA au Canada blanchiraient des centaines de millions de dollars canadiens chaque année.

En 2019, le gouvernement du Canada a modifié le *Code criminel* en ce qui concerne les infractions liées au blanchiment d'argent. Au paragraphe 462.31(1), Recyclage des produits de la criminalité, l'infraction a été élargie afin d'englober non seulement les cas où une personne sait ou croit que les biens ou leurs produits utilisés, transférés, transportés ou autrement traités ont été obtenus par la perpétration d'une infraction, mais aussi les cas des personnes qui ne s'en soucient pas. Par le passé, le fait qu'une personne devait connaître ou croire connaître la provenance des biens faisait en sorte qu'il était très difficile de poursuivre un PBA puisqu'il n'avait pas de lien direct avec l'infraction sous-jacente. La modification législative offre aux organismes d'application de la loi et aux procureurs un autre moyen de contrer le rôle complexe et changeant de ces PBA.

Certains groupes basés en Colombie-Britannique, en Ontario et au Québec blanchissent leurs propres produits de la criminalité, mais offrent aussi leurs services à d'autres groupes criminels qui entretiennent des liens avec l'Asie, surtout liés aux marchés des précurseurs chimiques et des drogues synthétiques.

Méthodes de blanchiment d'argent

Pratiquement tous les aspects de l'économie légitime, y compris les institutions financières, peuvent être exploités ou utilisés à mauvais escient pour blanchir des fonds. Les GCO emploient différentes méthodes pour blanchir des produits de la criminalité et se soustraire aux mesures de lutte contre le blanchiment d'argent. Les stratagèmes les plus complexes peuvent comprendre les trois étapes du processus susmentionné, réalisées grâce à des ETF, à des SITF et au BATC.

Dans le rapport de 2018 intitulé *Independent Review of Money Laundering in British Columbia*, Peter German et ses associés ont évalué de principales méthodes de blanchiment d'argent, incluant le blanchiment dans les casinos, dans le secteur immobilier et dans le secteur des véhicules de luxe. Les conclusions de l'examen indépendant ont donné lieu à la création de la commission d'enquête sur le blanchiment d'argent en Colombie-Britannique, la commission Cullen, qui se poursuit en 2020.

Des GCO et des PBA aux degrés d'expertise variables parviennent à blanchir des fonds grâce au secteur immobilier, aux casinos, aux entreprises privées, à la cryptomonnaie et à la contrebande d'argent liquide. Certaines méthodes plus complexes, comme le BATC ou des stratagèmes impliquant des ententes financières compliquées, nécessitent souvent l'aide de PBA ou d'autres professionnels comme des comptables, des banquiers et des avocats.

Les 176 groupes qui font du blanchiment d'argent utilisent principalement des entreprises du secteur privé, des ETF et des SITF, des casinos et les jeux d'argent[4], le secteur immobilier et la cryptomonnaie. Les GCO et autres criminels peuvent employer plus d'une méthode pour blanchir des fonds à tout moment, selon le montant des fonds illicites à recycler et l'accès aux différentes méthodes.

Entreprises du secteur privé

Des entreprises du secteur privé sont utilisées de différentes façons pour blanchir des fonds : on peut mélanger des produits de la criminalité aux rentrées de fonds légitimes, falsifier des reçus et des factures, payer des employés en argent comptant, utiliser des comptes d'entreprise pour acheter des biens (immobilier ou autres biens de grande valeur) et ainsi camoufler davantage la provenance des fonds, utiliser des prête-noms et des entreprises fictives pour

[4] Aux fins de cette évaluation, les méthodes de jeu légales et illégales, comme l'utilisation des casinos et des maisons de jeux illégales, ont été regroupées en une seule catégorie. Ceci est le résultat des lacunes dans les rapports concernant les types spécifiques de jeux utilisés, de sorte qu'une différenciation n'a pas pu être faite.

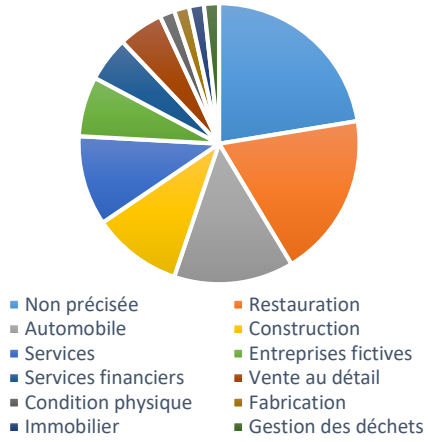
éloigner les opérations des bénéficiaires effectifs, et offrir des services financiers ou de prêt au moyen des produits de la criminalité. Des 176 GCO impliqués dans le blanchiment d'argent, environ 28 p. 100 (50) auraient recours à des entreprises du secteur privé pour faciliter le blanchiment de produits de la criminalité ou le camouflage de leur origine.

Le vaste rayon d'action des entreprises du secteur privé au Canada donne au crime organisé diverses possibilités pour dissimuler les activités de blanchiment et constitue aussi un défi pour la collectivité de l'application de la loi, qui doit déterminer quelles entreprises font du blanchiment d'argent, directement ou indirectement. Le recours à des prête-noms complique aussi l'établissement de liens entre des entreprises et des groupes.

Selon la Direction générale de la petite entreprise d'Innovation, Sciences et Développement économique Canada (ISDE), 1,18 million d'établissements employeurs au Canada fournissent de l'emploi à environ 11,9 millions de personnes en date de décembre 2017. La majorité de ces établissements (1,15 million ou 97,9 p. 100) sont de petites entreprises qui emploient moins de 100 personnes : en fait, plus de la moitié (53,8 p. 100) comptent entre un et quatre employés.

Le nombre d'entreprises auxquelles sont reliés des GCO ou dans lesquelles ils ont une influence serait sous-estimé. Selon les observations liées aux 176 GCO impliqués dans le blanchiment d'argent, les entreprises privées qui faciliteraient le plus le processus feraient partie des secteurs de la restauration (p. ex. restaurants et bars), de l'automobile (p. ex. vente et réparation de véhicules) et de la construction (p. ex. nouvelles constructions et rénovations). La **figure 7** illustre les types d'entreprises du secteur privé utilisées pour blanchir des produits de la criminalité.

Figure 7 – Types d'entreprises du secteur privé utilisées par des GCO pour blanchir de l'argent en 2019



Entreprises de transfert de fonds

Le CANAFE supervise les ETF enregistrées au Canada et les définit comme des entreprises qui offrent des services de change de devises étrangères et de virement de fonds, qui permettent d'émettre ou de recevoir des mandats bancaires, des chèques de voyage et autres produits semblables et qui traitent la monnaie virtuelle (la surveillance de ce dernier élément effective à compter du 1er juin 2020). Ces entreprises sont réglementées et doivent s'enregistrer avant d'exercer leurs activités. En mars 2019, 1101 ETF étaient enregistrées auprès du CANAFE.

Il y a deux types d'ETF au Canada : des sociétés nationales qui comptent de nombreux agents qui peuvent accéder à des centaines de milliers de sites dans le monde, effectuer un grand nombre d'opérations et offrir divers services, et des sociétés locales qui effectuent des transactions dans des régions géographiques précises, qui sont relativement petites et souvent familiales. Comme les ETF sont des entreprises nécessitant des liquidités importantes, elles peuvent faciliter le placement de fonds illicites dans le système financier légitime. Deux des plus grandes ETF nationales au Canada transmettent généralement de l'argent par virement télégraphique et compteraient, respectivement, plus de 5000 et 2500 succursales au pays. Les ETF locales, de petite taille, ont un nombre limité de succursales et font normalement partie d'un SITF.

Les SITF sont des systèmes parallèles de remise de fonds (communément appelés des réseaux *hawala*, *hundi* et *fei ch'ien*) utilisés partout dans le monde, dans des secteurs où l'accès à des services bancaires traditionnels est limité. Les SITF permettent aux clients de transférer la valeur voulue sans que les fonds soient physiquement transférés d'un pays à un autre. Comme les ETF, les SITF doivent être enregistrés auprès du CANAFE et respecter les obligations en vertu de la LRPCFAT.

Les GCO exploitent les ETF légitimes aux fins du blanchiment d'argent en utilisant l'infiltration et la corruption ou en les rendant complices si elles font fi des indices de criminalité et acceptent de faire des transactions à partir de fonds qu'elles soupçonnent de provenir d'activités criminelles. Plus préoccupantes encore sont les ETF qui appartiennent à des GCO ou sont contrôlées par ceux-ci, parce qu'elles peuvent blanchir des montants importants d'argent et faciliter des transactions illégales pour le paiement d'activités criminelles à l'étranger, comme l'importation de drogues.

Casinos et jeu illégal

Les casinos gèrent des montants d'argent considérables et sont essentiellement des entreprises où les transactions se font en espèces, mais ils ne sont pas considérés comme des ETF. Ils sont susceptibles d'être exploités par des criminels qui cherchent à blanchir les produits de leurs crimes et certains sont effectivement exploités à cette fin. Bien que les casinos soient tenus de signaler au CANAFE les transactions importantes en espèces et toute opération douteuse, quelle qu'en soit la valeur, le volume de la monnaie en circulation dans les casinos permet de bien dissimuler les fonds illicites.

On estime que 18 des GCO évalués en 2019 utilisent des casinos ou le jeu illégal pour blanchir les produits de leurs crimes. Les criminels blanchissent des fonds dans les casinos en achetant des jetons avec des produits de la criminalité sous forme d'argent comptant, de traites de banque ou d'autres instruments financiers. Après avoir joué avec les jetons, qu'ils aient fait des gains ou non, les individus encaissent leurs jetons sous forme de dépôt sur leur compte de fonds de jeu, de chèque de casino ou d'argent comptant avec un reçu du casino et obtiennent donc une preuve de légitimité, puisque les fonds représentent des gains de jeu, à moins d'avoir été identifiés autrement par le casino (p. ex. un retour de fonds et non des gains de jeu).

La réglementation a changé dans les casinos de la Colombie-Britannique en janvier 2018 en vue de prévenir et d'éviter le blanchiment d'argent dans ces établissements. On a notamment modifié la façon de vérifier la provenance des fonds en tranches de 10 000 $CAN par période de 24 heures et ajouté une mention sur les chèques émis par le casino qui ne représentent pas des gains (c'est-à-dire « un retour de fonds et non des gains de jeu »). L'impact de ces changements réglementaires est inconnu pour le moment. On soupçonne que cette méthode d'utilisation de casinos pour blanchir l'argent a potentiellement évolué et / ou est utilisée dans des casinos dans d'autres provinces canadiennes, bien que les renseignements sur ces développements n'aient pas encore été établis.

Immobilier

(La présente section porte sur l'utilisation du secteur de l'immobilier pour faciliter le blanchiment d'argent. La section consacrée à la fraude immobilière se trouve à la page 26.)

Des criminels exploitent le marché de l'immobilier aux fins du blanchiment d'argent en utilisant des produits de la criminalité pour acheter des propriétés, souvent après que les fonds illicites ont passé les étapes du placement et de la dispersion, afin d'en camoufler la provenance criminelle. Les biens immobiliers constituent un moyen intéressant d'investir des fonds illicites parce qu'ils offrent un endroit où habiter, un investissement de grande valeur relativement sûr et un lieu d'où on peut exercer d'autres activités criminelles (repaires de BMHL, casinos clandestins, maisons de prostitution, sites de production ou de trafic de drogue).

Le blanchiment d'argent par les biens immobiliers nécessite le recours à différents stratagèmes liés à l'hypothèque et à d'autres prêts qui permettent d'utiliser des produits de la criminalité pour acheter des propriétés. Les méthodes utilisées comprennent l'achat de propriétés, le refinancement ou le paiement de prêts hypothécaires ou d'autres prêts au moyen des produits de la criminalité, ainsi que la manipulation de la valeur des propriétés (aussi considérée comme une fraude) et l'obtention de prêts en fonction d'une valeur surévaluée qui sont remboursés au moyen de produits de la criminalité. Les biens immobiliers achetés servent à blanchir des fonds lorsque les propriétaires déclarent que des produits de la criminalité constituent un revenu de location ou lorsqu'ils font faire des rénovations. Selon la complexité de la transaction, les criminels peuvent solliciter l'aide de professionnels (évaluateurs, agents immobiliers, comptables, avocats ou notaires) corrompus ou utilisés à leur insu pour effectuer la transaction. Les connaissances et compétences spécialisées de ces fournisseurs de services permettent de camoufler la provenance des fonds et la propriété effective.

La transparence inadéquate entourant la propriété effective au Canada est un facilitateur important du blanchiment d'argent par les biens immobiliers, car la possibilité pour des entreprises, des partenariats, des fiducies et des prête-noms d'être propriétaires de biens immobiliers permet de dissimuler l'identité des individus qui ont le véritable contrôle du bien en question.

BLANCHIMENT FONDÉ SUR LES TRANSACTIONS COMMERCIALES

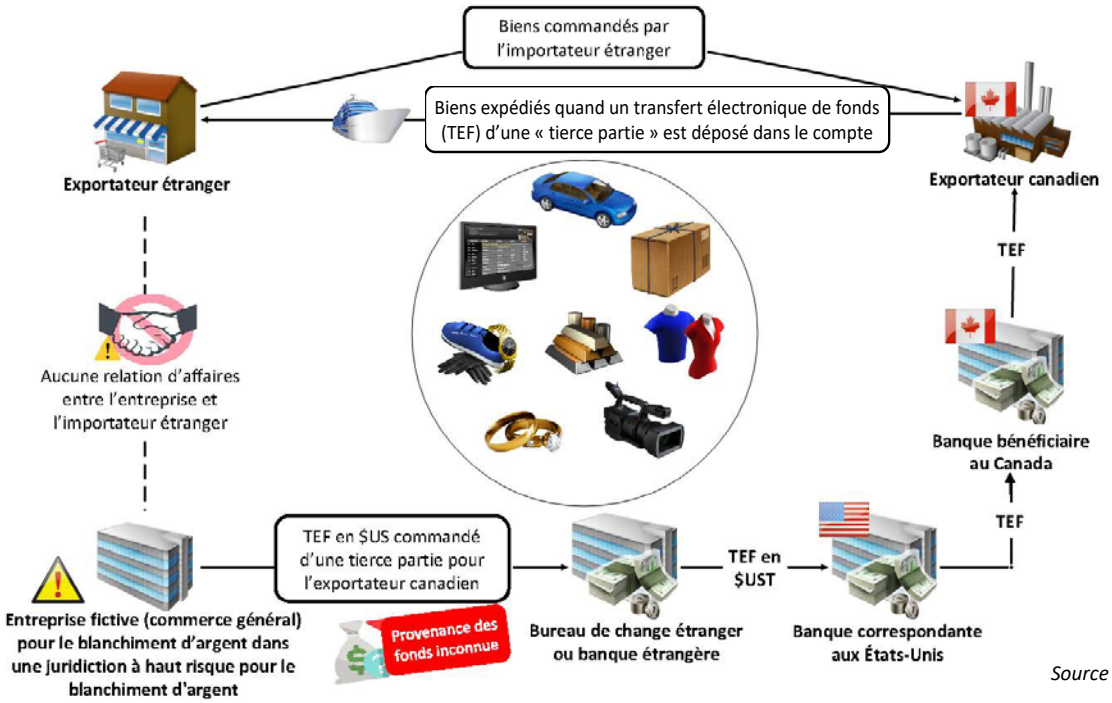
Faits saillants

- Le blanchiment d'argent fondé sur les transactions commerciales (BATC) permet de déplacer des produits de la criminalité qui se chiffreraient à plusieurs centaines de millions de dollars au Canada, mais serait sous-estimé en raison de la complexité et de la portée internationale des ententes commerciales qui sont utilisées.
- Les PBA canadiens exercent des activités importantes de BATC pour des clients à l'étranger. Toutefois, on ne connaît pas tous les détails sur la portée des stratagèmes employés par des GCO canadiens bien établis.
- Comme les mesures de lutte contre le blanchiment d'argent ciblent d'autres méthodes de blanchiment, les PBA utiliseront probablement encore plus le BATC.
- Les paiements de transactions commerciales par des sociétés d'import-export qui sont des tiers indépendants dans des pays très propices au blanchiment d'argent représentent un risque important dans les stratagèmes de BATC.

Analyse du marché

On entend par BATC le processus qui consiste à déplacer des fonds illicites dans le cadre de transactions commerciales afin d'en dissimuler la provenance. Les criminels utilisent des produits de la criminalité pour acheter des biens dans un marché commercial légitime et concluent des ententes compliquées pour justifier le transfert de fonds entre parties et d'un territoire à un autre. À l'aide de fausses factures et déclarations de douanes, de paiements effectués par des sociétés tierces indépendantes et de systèmes clandestins de transfert de fonds, le BATC est particulièrement utile pour rapatrier des fonds dans des pays source de drogues tout en contournant les restrictions liées à la fuite de capitaux et en évitant les sanctions connexes. Des biens de toutes sortes peuvent être utilisés dans un stratagème de BATC, mais les appareils électroniques, les véhicules, le textile, les pierres précieuses et les métaux précieux sont souvent employés. Dans de nombreux cas, aucun bien physique n'est échangé, les factures frauduleuses justifiant et couvrant les transferts de fonds transnationaux entre entreprises. Le commerce intérieur peut aussi être utilisé à des fins de blanchiment d'argent, mais le BATC est surtout axé sur l'exploitation de marchés étrangers, ce qui permet aux fournisseurs de services de profiter de la complexité des ententes commerciales complexes qui touchent plusieurs territoires (voir la **figure 8**).

Figure 8 – Paiements de tiers : dispersion et intégration de fonds illicites étrangers dans l'économie canadienne



Source : GRC

Le ministère des Finances du Canada a déterminé que la fraude commerciale, qui comprend le BATC, représentait une menace très élevée dans son *Évaluation des risques inhérents au recyclage des produits de la criminalité et au financement des activités terroristes au Canada* de 2015. Selon les renseignements recueillis dans le cadre d'enquêtes en cours, de divulgations au CANAFE et de recherches dans les sources ouvertes, les PBA canadiens et les GCO transnationaux utiliseraient de plus en plus ce type de blanchiment d'argent depuis cinq ans.

Capacités et vulnérabilités

Les PBA sont généralement dissociés des infractions sous-jacentes qui ont généré les produits de la criminalité au Canada ou à l'étranger. Les GCO et ces PBA ont recours à diverses méthodes de BATC, selon la situation. Des renseignements frauduleux aux douanes (fraude douanière), des paiements de tiers (fraude électronique) et l'échange de pesos sur le marché noir sont des exemples de stratagèmes courants. Bien que le BATC puisse être effectué n'importe où, les sociétés commerciales et entreprises du Canada utilisées sont essentiellement regroupées dans les grands centres de logistique et de commerce du pays, notamment Toronto, Vancouver, Montréal et Halifax.

Le thème commun du BATC qui consiste à divulguer de faux renseignements aux douanes constitue surtout de la fraude liée à la facturation et aux déclarations en douane. Dans les stratagèmes d'envois fictifs, des fonds sont virés et tous les documents à l'appui existent, mais aucun bien n'est réellement expédié et aucun service n'est rendu. Dans le cas des stratagèmes de surfacturation ou de sous-facturation, des biens sont expédiés, mais leur valeur réelle est supérieure ou inférieure au montant facturé. Ces faux renseignements permettent de camoufler le transfert de fonds et, dans les cas de sous-facturation, de masquer le revenu additionnel associé à la vente des biens. Plus simplement, des biens de grande valeur peuvent être achetés avec des produits de la criminalité, exportés puis vendus à l'étranger.

L'échange de pesos sur le marché noir est employé par des GCO transnationaux, comme des cartels de drogue mexicains ou sud-américains, pour rapatrier leurs profits, souvent des États-Unis. Plusieurs méthodes font partie de cette catégorie, qui comporte généralement des dépôts structurés en espèces en devises américaines, suivis d'opérations par des importateurs mexicains ou sud-américains qui achètent ces fonds américains en pesos auprès de courtiers complices. L'importateur utilise les fonds américains pour acheter des biens qui sont expédiés dans son pays et le courtier envoie les pesos de l'importateur aux cartels. Des liens ont été établis entre le Canada et un stratagème d'échange de pesos sur le marché noir : des produits de la criminalité présumés ont été envoyés des États-Unis ou de l'Amérique du Sud à des sociétés commerciales canadiennes qui utilisaient les fonds pour acheter des biens auprès d'exportateurs à l'étranger.

CRYPTOMONNAIE

Faits saillants

- La connaissance et l'utilisation de la cryptomonnaie ont augmenté de manière constante au cours des trois dernières années, autant chez les citoyens que chez les GCO du Canada.
- La cryptomonnaie est souvent utilisée comme moyen de paiement pour la fraude par marketing de masse et les achats sur le Web profond, mais constitue aussi un outil intéressant pour blanchir des produits de la criminalité.
- Le recours à des outils et des services d'anonymat, comme des services de mixage (*mixers* et *tumblers*), qui permettent de camoufler l'origine des transactions de cryptomonnaie, a triplé au cours de la dernière année.
- Des modifications récentes à la réglementation canadienne pour lutter contre le blanchiment d'argent feront en sorte que les complices qui échangent de la cryptomonnaie à des fins criminelles devront adopter de nouvelles méthodes pour éviter que les transactions soient déclarées aux groupes du renseignement financier, ce qui pourrait en pousser plusieurs à déplacer leurs activités à l'étranger.

Analyse du marché

Les cryptomonnaies sont des biens numériques décentralisés qui peuvent être échangés contre de la monnaie émise par le gouvernement (à cours forcé), transférés d'une personne à une autre, ou échangés contre d'autres devises virtuelles. La toute première devise de cryptomonnaie qui a été créée, le bitcoin, compte pour près de 70 p. 100 du marché. Elle demeure la devise la plus utilisée dans le monde, mais il en existe plus de 2500 autres.

La connaissance de cette technologie et l'intérêt qu'elle suscite ont augmenté de façon constante depuis la création du bitcoin en 2009. En 2019, 89 p. 100 des Canadiens interrogés avaient entendu parler de Bitcoin, alors que ce pourcentage était de 62 en 2016. Le bitcoin peut être utilisé pour faire des achats au Canada dans certains cafés et restaurants, chez certains détaillants de matériel électronique et sur certains sites Web de commerce électronique. Les consommateurs peuvent acheter de la cryptomonnaie avec de la monnaie à cours forcé à des bureaux de change de cryptomonnaie, à des guichets automatiques de cryptomonnaie ou sur des plateformes informelles d'échange pair-à-pair (*peer-to-peer*). Comme le reste de la population, les criminels au Canada utilisent de plus en plus les cryptomonnaies. Ces devises sont intéressantes pour eux, car les opérations sont confidentielles et il est difficile pour les organismes d'application de la loi d'identifier les parties concernées.

Le recours aux services de mixage, des outils qui permettent de masquer la provenance des transactions en mélangeant différents flux de crypto-monnaie potentiellement identifiables, a grandement augmenté dans la dernière année, probablement parce que les organismes d'application de la loi ont une meilleure capacité pour l'analyse judiciaire de la chaîne de blocs, le système de tenue de dossiers de la cryptomonnaie. Dans le cas de plusieurs cryptomonnaies, y compris le bitcoin, toutes les transactions sont enregistrées dans un grand livre accessible au public. Le processus de mixage consiste à rassembler les cryptomonnaies de plusieurs utilisateurs avant de les transférer, ce qui complique grandement le travail des organismes d'application de la loi qui veulent associer des transactions à des individus. Une analyse menée en avril 2019 révèle que plus de 4 p. 100 de toutes les transactions en bitcoins étaient mixées, ce qui représente une augmentation de 300 p. 100 par rapport aux données de juillet 2018, soit neuf mois plus tôt. D'autres cryptomonnaies, connues sous le nom anglais de « *privacy coins* » pour l'anonymat qu'elles procurent, permettent de masquer l'origine des transactions car celles-ci n'ont pas à être inscrites dans un grand livre accessible au public. À l'aide des services de mixage, de ces cryptomonnaies privées ou des deux, les criminels peuvent déplacer d'importantes sommes de cryptomonnaies en profitant d'une solide protection de leur vie privée, sans que leurs transactions soient déclarées comme elles l'auraient été si elles avaient passé par le secteur financier traditionnel.

Capacités et vulnérabilités

La cryptomonnaie a des répercussions importantes sur les Canadiens quand elle est utilisée à des fins criminelles. Le bitcoin et d'autres devises sont la méthode de paiement privilégiée par les fraudeurs par marketing de masse. Les

transactions de cryptomonnaie sont irréversibles, ce qui complique les tentatives de recouvrement après le signalement d'une fraude. Les cryptomonnaies sont aussi pleinement intégrées au modèle de fonctionnement du trafic de contrebande sur le Web profond. Selon le rapport de 2019 d'EUROPOL intitulé *Internet Organized Crime Threat Assessment*, le bitcoin était la cryptomonnaie la plus souvent utilisée dans les opérations de marché dans le Web profond, représentant des dépenses de plus d'un milliard de dollars américains.

En tant qu'outil de blanchiment d'argent, la cryptomonnaie permet de transférer d'importantes sommes d'argent à l'abri de la surveillance du secteur financier traditionnel et des exigences de signalement liées à d'autres types d'opérations. Le pseudo-anonymat inhérent au processus de la cryptomonnaie fait partie de son attrait. Bien que les chaînes de blocs n'enregistrent pas les noms des individus impliqués, toutes les opérations laissent un indice important que peuvent évaluer les organismes d'application de la loi. Les données du grand livre public distribué par Bitcoin peuvent être analysées au moyen de divers outils qui facilitent l'identification des parties ayant participé aux transferts.

Les bureaux de change de cryptomonnaies représentent une importante méthode de placement des produits de la criminalité en devises numériques. Ces entreprises facilitent, en ligne ou en personne, les opérations et la conversion de monnaie à cours forcé en cryptomonnaie de même que l'échange d'un type de cryptomonnaie à un autre. De tels échanges camouflent la source originale des fonds et peuvent en compliquer le suivi.

Il y a plus de 730 guichets automatiques de cryptomonnaie au Canada, alors qu'il n'y en avait que 205 en 2017. Ces guichets peuvent être utilisés par des criminels pour déposer des fonds illicites en espèces et les convertir en bitcoins ou en une autre devise numérique. Plusieurs de ces guichets ne nécessitent aucune preuve d'identité. Les guichets automatiques de cryptomonnaie ont différentes limites en ce qui concerne le montant des dépôts et des retraits, le plus souvent en deçà de 10 000 $CAN. Il peut aussi être avantageux pour les criminels de posséder ou de gérer ces guichets puisqu'un criminel qui a le contrôle d'un guichet automatique peut y déposer des sommes importantes de produits de la criminalité, pour ensuite recevoir un paiement électronique légitime.

Des GCO bien établis de toutes sortes (depuis les BMHL jusqu'aux GCO structurés comme la mafia, ainsi que les PBA qui les appuient) utiliseraient la cryptomonnaie à des fins criminelles, notamment le blanchiment de produits de la criminalité et le transfert de fonds pour payer des drogues et des activités illégales. Des groupes entretenant des liens avec l'Asie utilisent vraisemblablement des bitcoins pour déplacer d'argent d'un pays à un autre, puisque c'est une méthode reconnue pour éviter les limites à la fuite des capitaux.

La cryptomonnaie est une méthode de paiement répandue pour la fraude par marketing de masse. Le CANAFE a signalé une hausse importante des déclarations d'opérations douteuses liées aux cryptomonnaies et à la fraude en 2017 et en 2018.

Répercussions sur les organismes canadiens de l'application de la loi

Le gouvernement du Canada a modifié les règlements associés à la LRPCFAT en juillet 2019 afin de réglementer les entités qui se livrent au commerce de la monnaie virtuelle et de mettre à jour les exigences liées aux déclarations et à la tenue de dossiers relatifs aux opérations en monnaie virtuelle. Les changements, qui devront être appliqués de façon progressive à compter de juin 2020, devraient avoir une grande incidence sur le fonctionnement des bureaux de change de cryptomonnaies. En vertu des nouveaux règlements, les bureaux de change de cryptomonnaie seront considérés comme des ETF et devront s'inscrire auprès du CANAFE, mettre en place des programmes de conformité et signaler les opérations douteuses. Ces modifications réglementaires visent à renforcer la lutte contre le blanchiment d'argent au Canada, conformément aux lignes directrices du Groupe d'action financière international.

Les modifications à la LRPCFAT auront une incidence importante sur la façon dont les criminels acquièrent et transfèrent la cryptomonnaie. Les criminels sont au courant de la règle de « Know Your Customer » (KYC), la collecte d'informations identifiables des clients pour permettre des enregistrements attribuables des transactions financières.

En 2018, le bureau de change américain ShapeShift a observé une réduction importante de sa clientèle et de ses revenus quand il a commencé à recueillir des renseignements sur l'identité de ses clients. Compte tenu du resserrement des règlements sur les échanges au pays, les criminels à la recherche de cryptomonnaie utilisent probablement l'échange pair-à-pair, souvent annoncé en ligne, et les PBA profitent vraisemblablement de la demande dans ce domaine nouvellement réglementé pour offrir des services de rechange. Les rapports du CANAFE de 2015 à 2018 révèlent que les activités dans les comptes d'entreprises soupçonnées de se livrer au blanchiment d'argent par la cryptomonnaie ne correspondaient pas à la nature officielle de ces entreprises. Les entreprises qui prétendaient opérer dans divers secteurs utilisaient leurs comptes comme canaux intermédiaires pour acheter et vendre de la monnaie virtuelle.

Bien que la modification de la réglementation soit une étape positive dans la gestion de l'utilisation de la cryptomonnaie à mauvais escient, plusieurs obstacles du point de vue de l'application de la loi demeurent. Les cryptomonnaies sont décentralisées et il n'y a aucun point de contact central responsable de l'accès à cette forme de monnaie ou de la surveillance des transactions. Comme il est le cas pour bien des crimes ayant un élément cybernétique, les organismes d'application de la loi doivent composer avec des défis liés aux territoires de compétence lorsqu'ils doivent établir des liens à l'étranger.

FRAUDE PAR MARKETING DE MASSE

La fraude par marketing de masse englobe les stratagèmes de fraude pour lesquels on utilise des moyens de communication de masse (téléphone, Internet, envois postaux, télévision, radio, rencontre en personne) pour frauder plusieurs personnes sur au moins un territoire. La présente section porte sur cinq catégories de stratagèmes importantes : les stratagèmes liés aux services du gouvernement, le vol d'identité et l'hameçonnage, les stratagèmes de rencontre, le recours aux rançongiciels et les stratagèmes ciblant les personnes âgées.

Stratagèmes liés aux services du gouvernement

Dans les stratagèmes liés aux services du gouvernement, qui sont une forme de télémarketing frauduleux, un individu (ou un groupe) se fait passer pour un représentant du gouvernement pour amener une victime à dévoiler des renseignements financiers ou personnels de nature délicate afin de voler son argent ou son identité. Dans bien des cas, les fraudeurs ont recours à l'extorsion pour mener à bien leur stratagème. Ils menacent leurs victimes de graves conséquences financières ou judiciaires si elles ne font pas immédiatement ce qui leur est demandé et exigent un paiement sous la forme d'un virement Interac, en cryptomonnaie (p. ex. bitcoins), ou à l'aide d'une carte de crédit prépayée ou d'une carte-cadeau. Ces stratagèmes minent la confiance du public dans les institutions gouvernementales et les organismes d'application de la loi et peuvent accentuer la méfiance de bien des citoyens, surtout ceux qui font partie des groupes vulnérables.

Les stratagèmes liés aux services du gouvernement étaient par le passé exécutés par téléphone et par courriel, mais les fraudeurs utilisent de plus en plus d'outils, notamment la messagerie texte ou les médias sociaux (p. ex. Facebook Messenger ou WhatsApp) pour communiquer avec leurs victimes. On a d'ailleurs récemment remarqué une augmentation des stratagèmes où les criminels usurpent un numéro de téléphone légitime du gouvernement lorsqu'ils entrent en contact avec leurs victimes. Le **tableau 2** présente certains des stratagèmes les plus courants au Canada. Bien que plusieurs stratagèmes visent à escroquer l'argent des victimes, celui de Service Canada, qui est utilisé plus souvent ces derniers temps, est particulièrement préoccupant parce que la divulgation involontaire du numéro d'assurance sociale (NAS) et d'autres renseignements personnels, comme le nom et l'adresse, donnent souvent lieu au vol d'identité.

Tableau 2 – Types de stratagèmes récents

Agence du revenu du Canada (déclaration de revenus) Les fraudeurs convainquent les victimes de payer une fausse dette ou leur offrent un remboursement et leur demandent le numéro de leurs comptes bancaires et d'autres renseignements financiers.
Service Canada (numéro d'assurance sociale) Les fraudeurs prétendent que le NAS d'une personne a été annulé, compromis ou associé à un acte criminel et exigent des frais pour régler le problème (étroitement lié au vol d'identité).
Immigration, Réfugiés et Citoyenneté Canada (fraude liée à l'immigration) Les fraudeurs allèguent qu'un immigrant ou un individu qui cherche à obtenir la citoyenneté n'a pas rempli ou présenté correctement ses documents d'immigration et lui imposent des frais pour éviter l'expulsion.

Très peu de GCO canadiens auraient été impliqués dans ce type de stratagème dans les dernières années : quatre seulement ont été signalés en 2019. Les Canadiens sont principalement ciblés par des fraudeurs qui exploitent des entreprises de vente sous pression à l'étranger et dont l'extorsion est le seul objectif. Une enquête conjuguée de la GRC et d'organismes d'application de la loi en Inde ciblant des centres d'appels en Inde où on commettait de la fraude liée à l'Agence du revenu du Canada (ARC), a donné lieu à l'arrestation de mules présumées au Canada et d'opérateurs de centres d'appels en Inde en mars 2020. Les nouveaux citoyens et les résidents qui espèrent devenir citoyens sont particulièrement susceptibles d'être victimes de ces stratagèmes, car ils ne connaissent pas bien les pratiques gouvernementales légitimes. En 2018, par exemple, les autorités des États-Unis ont perturbé un stratagème lié à l'Internal Revenue Service mené à partir de l'Inde, dans le cadre duquel les fraudeurs se faisaient passer pour des représentants du gouvernement et menaçaient de faire arrêter ou d'expulser leurs victimes si elles ne versaient pas les paiements demandés. Plus de 15 000 personnes ont perdu des centaines de millions de dollars américains et plus de 50 000 personnes ont vu leurs renseignements personnels être utilisés à mauvais escient.

Vol d'identité et hameçonnage

Selon le CAFC, près de 2000 Canadiens auraient été victimes d'un vol d'identité en 2019 et auraient perdu au total plus de 506 000 $CAN. Cela représente une nette augmentation par rapport à 2017, où un peu plus de 1500 Canadiens avaient été victimes de fraude et auraient perdu près de 269 000 $CAN. Les victimes du vol d'identité appartiennent à toutes les sphères de la société, quel que soit leur revenu ou leur âge.

Plusieurs stratagèmes différents sont employés pour voler l'identité des gens. Une méthode courante implique l'hameçonnage, par lequel les criminels communiquent avec des individus tout en prétendant appartenir à des entités de bonne réputation afin d'induire la divulgation d'informations personnelles (voir le **tableau 3** pour des types d'hameçonnage). L'hameçonnage peut prendre la forme de contraventions frauduleuses, d'appels de service non sollicités, de services de dépannage informatique ou d'offres de voyages ou de vacances, entre autres. Le nombre de signalements de cas d'hameçonnage et la valeur des pertes qui y sont associées ont augmenté au cours des trois dernières années. L'hameçonnage demeure l'un des stratagèmes les plus courants liés au vol d'identité. Le harponnage serait devenu le type de stratagème de vol d'identité le plus lucratif en 2019, ayant entraîné des pertes de plus de 21,4 millions de dollars canadiens.

Une tendance signalée récemment touche l'échange de cartes SIM, où les fraudeurs se font passer pour le représentant d'un fournisseur de téléphonie mobile et utilisent les renseignements personnels de l'abonné pour signaler la perte ou le vol du téléphone. Le numéro de téléphone est ensuite lié à une nouvelle carte SIM et un nouvel appareil contrôlé par le fraudeur, qui peut accéder aux applications et réinitialiser les mots de passe. Si un compte bancaire en ligne est associé au numéro de téléphone ou à l'adresse courriel de la victime, le fraudeur peut obtenir un nouveau code de vérification et prendre le contrôle du compte.

Tableau 3 – Types de fraudes par hameçonnage

Hameçonnage par courriel Cible un grand nombre de personnes au hasard
Harponnage Attaque ciblée contre une seule personne
Hameçonnage visant les cadres Attaque ciblée contre des employés haut placés, comme les PDG

Douze des GCO évalués en 2019 seraient impliqués dans le vol d'identité au Canada. La majorité de ces groupes sont basés en Colombie-Britannique et près de la moitié d'entre eux entretiennent des liens à l'étranger. Certains membres d'un groupe entretiennent des liens directs au Nigéria, à partir d'où des stratagèmes d'hameçonnage visent des Canadiens depuis longtemps. Outre ces GCO, d'autres criminels utilisent leur expertise pour commettre des vols d'identité, comme le démontrent les signalements récents de vol de données par des employés d'institutions financières. En 2019, le groupe Desjardins a été victime de fraude lorsqu'un employé a volé les renseignements personnels de 4,2 millions de clients. Des clients de Capital One au Canada et aux États-Unis se sont aussi fait voler leurs renseignements personnels par un pirate, un ancien ingénieur en logiciel d'Amazon. Tandis que l'incident de Desjardins met en évidence les menaces internes potentielles pour les institutions financières, l'incident de Capital One montre à quel point ces sociétés sont vulnérables aux attaques criminelles ou malveillantes de l'extérieur.

Stratagèmes de rencontre

Selon les signalements au CAFC en 2018 et 2019, les victimes auraient perdu plus de 24 millions de dollars canadiens à cause de stratagèmes de rencontre. Les pertes réelles sont probablement bien plus élevées, puisque seulement cinq pour cent des incidents seraient signalés. De 15 000 à 20 000 Canadiens auraient subi des pertes financières attribuables à des stratagèmes de rencontre en 2018, alors que moins de 1000 incidents ont été déclarés.

Stratagème de rencontre type

Les victimes sont attirées dans une fausse relation avec un fraudeur, qui se sert souvent des renseignements qu'elles ont affichés en ligne. Une fois la confiance établie, une situation d'urgence est inventée et les fraudeurs ont un besoin pressant d'argent. En jouant sur les émotions des victimes, ils leur extorquent de l'argent.

Les criminels impliqués dans les stratagèmes de rencontre sont souvent aussi impliqués dans d'autres types de fraudes. Les transactions permettant de blanchir de l'argent dans le cadre de ces stratagèmes et le recours à des mules pour faciliter des crimes semblent indiquer que les GCO pourraient travailler ensemble pour mener à bien ces stratagèmes, parfois à l'échelle internationale. Par exemple, on estime qu'un GCO transnational basé au Nigéria vole

de 100 à 300 millions de dollars américains par année en Amérique du Nord. Ce GCO, qui a une présence dans au moins 26 pays dont le Canada, se livre principalement à la fraude (stratagèmes de rencontre et opérations de contrefaçon) et au blanchiment d'argent un peu partout au Canada. Les stratagèmes de rencontre représentent environ 50 p. 100 de ses activités criminelles. Le groupe recrute de jeunes hommes instruits et mènerait ses stratagèmes en passant par trois étapes : attirer la victime, établir et maintenir une fausse relation romantique avec elle, puis lui soutirer de l'argent. Le groupe se sert aussi de ses victimes en tant que mules pour blanchir de l'argent, normalement obtenu d'une autre victime ou activité criminelle, afin de se protéger davantage des mesures de répression.

On s'attend à une hausse des stratagèmes de rencontre dans les prochaines années, surtout à l'aide des médias sociaux (p. ex. sites de rencontre et de réseautage). Facebook se classe au premier rang des sites où des personnes tombent dans le piège des stratagèmes de rencontre, mais bien d'autres sont victimes à partir de sites de rencontre (p. ex. Match.com) et d'autres sites de réseautage social (p. ex. Instagram). Le nombre croissant d'applications sociales en ligne fait continuellement grossir le terrain de jeu des criminels.

Recours aux rançongiciels

On estime qu'au Canada, les particuliers et les institutions (y compris les entreprises, les universités, les banques, les hôpitaux et les organismes du gouvernement) seraient ciblés par des attaques de rançongiciel environ 3200 fois par jour, selon les données du CAFC. En moyenne, chaque attaque coûte entre un et trois millions de dollars canadiens, ce qui englobe les rançons payées et la perte de productivité. Bien que les rançongiciels ne représentent qu'une très faible proportion des extorsions signalées au CAFC, les pertes dues à ce type de fraude peuvent être importantes en termes d'argent et d'informations, et les chiffres ne représenteraient qu'une fraction du nombre réel d'incidents qui surviennent au Canada.

Définition de rançongiciel

Des criminels déploient des maliciels pour attaquer des réseaux informatiques en chiffrant des fichiers et en prenant des données en otage. Ils exigent un paiement, souvent en bitcoins, pour libérer les fichiers. Les ministères et les entreprises du secteur privé sont souvent ciblées en raison de la nature délicate des données en jeu et des gros profits à réaliser.
La plupart des victimes paient la rançon, car elle semble souvent moins coûteuse que la restauration de leur système, sauf que les fichiers sont souvent corrompus et irrécupérables et la perte de données est fréquente, même si la rançon est payée.

Des données peuvent être volées, ce qui peut donner lieu à des inquiétudes et des atteintes à la vie privée, et les systèmes informatiques compromis peuvent être la cible d'autres types de fraudes, comme le vol d'identité et l'extorsion, et représenter une menace pour l'infrastructure canadienne ou les opérations gouvernementales. Dans les attaques ciblant des institutions médicales, le rançongiciel qui détient des dossiers médicaux peut représenter de graves risques pour la santé, voire causer la mort. Dans un incident récent, le gouvernement du Nunavut a été ciblé par un rançongiciel qui a fait perdre aux citoyens l'accès aux services par Internet, aux allocations et à leurs rendez-vous médicaux. Cette perturbation temporaire des services a eu une incidence grave sur l'ordre public et sur les citoyens et a causé des dommages économiques. Dans un autre incident, un centre de santé offrant des services à environ 13 000 clients en Nouvelle-Écosse a été la cible d'un rançongiciel en 2018-2019 qui a entraîné la mise hors service de ses systèmes informatisés pendant plusieurs jours et des conséquences négatives pour de nombreux patients.

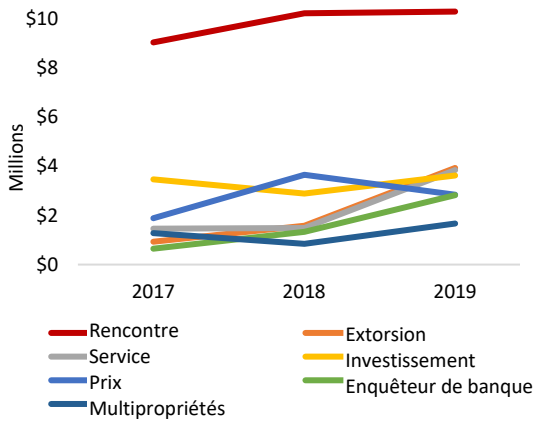
En 2019, les États-Unis ont été frappés par un nombre sans précédent de rançongiciels, qui ont touché 966 organismes du gouvernement ainsi que les secteurs des soins de santé et de l'éducation. Les services d'urgence ont été interrompus : les services de police n'avaient plus accès à leurs systèmes, les portes dans les prisons ne pouvaient plus être déverrouillées à distance et des dossiers médicaux ont été perdus.

Compte tenu de la nature cybernétique des rançongiciels, les criminels ne connaissent aucune limite géographique et peuvent se trouver n'importe où dans le monde. Aucun GCO canadien ne serait associé à ce type de stratagème, mais la complexité des enquêtes sur ce type d'activité ne permet pas aux organismes d'application de la loi d'avoir une juste appréciation de l'implication des groupes. Les rançongiciels demeureront probablement un cybercrime représentant une menace des plus préoccupantes, car ils permettent de réaliser d'importants profits.

Stratagèmes ciblant les personnes âgées

On s'attend à une hausse de la fraude ciblant les personnes de plus de 60 ans (souvent appelées personnes âgées ou aînés) au Canada étant donné que la population faisant partie de ce groupe d'âge augmente. Partout dans le monde, le nombre d'aînés augmente plus rapidement que les autres groupes d'âge. En 2016, on estimait déjà que les personnes âgées représentaient 17 p. 100 de la population au Canada. Le CAFC a enregistré plus de 14 000 plaintes touchant des personnes âgées en 2019, ce qui représente environ un quart de toutes les victimes canadiennes et des pertes de plus de 35 millions de dollars canadiens. Les principaux types de fraudes entraînant les plus grandes pertes pour les aînés sont les stratagèmes de rencontre, l'extorsion, la vente frauduleuse de services, les combines frauduleuses en matière d'investissements, les arnaques de l'enquêteur bancaire, les escroqueries de prix et les stratagèmes liés aux multipropriétés (voir la **figure 9**).

Figure 9 – Pertes financières chez les personnes âgées, selon le type d'arnaque, par année



Des GCO représentant une menace élevée, dont des membres des BMHL et des GCO dont la structure s'apparente à celle de la mafia, tirent profit indirectement de ces stratagèmes, parce qu'ils font partie d'une structure où une partie des profits leur sont versés par des coursiers et des GCO intermédiaires en échange d'une « protection ». Des criminels canadiens basés dans différentes provinces font partie d'un réseau international qui cible les Canadiens au moyen de stratagèmes qui visent normalement les aînés, y compris des arnaques qui consistent à se faire passer pour un représentant (p. ex. ARC, enquêteur de banque, technicien informatique). Les fraudeurs ont aussi commencé à se faire passer pour des policiers et à dire aux victimes qu'ils ont besoin d'aide pour une enquête sur de tels stratagèmes. Les criminels obtiennent un accès à distance à l'ordinateur des victimes et les amènent à transférer des milliers de dollars de leur compte bancaire dans le cadre de la fausse enquête.

Des GCO canadiens ciblent des aînés au Canada et aux États-Unis et continueront vraisemblablement à le faire compte tenu de leur succès et des profits élevés qu'ils réalisent. Les cibles américaines continueront de représenter un marché intéressant et lucratif en raison de la population nombreuse et de la valeur élevée du dollar américain. Dans les prochaines années, la proportion grandissante d'aînés et leur utilisation accrue d'Internet offriront de plus en plus de cibles aux criminels qui se livrent à ces stratagèmes.

FRAUDE EN VALEURS MOBILIÈRES

La fraude en valeurs mobilières englobe diverses activités illicites qui impliquent la tromperie ou la manipulation de marchés financiers. Parmi les stratagèmes les plus connus, mentionnons la distribution illégale, les délits d'initié et la manipulation du marché boursier (*pump and dump*), et en particulier les fraudes via les plateformes d'échange en ligne, les offres initiales de pièces de monnaie et les systèmes de Ponzi et Pyramid. La fraude en valeurs mobilières met en péril l'intégrité du marché financier et l'intérêt du public en raison des injustices ou des actes frauduleux visant des investisseurs, des sociétés ou le public.

Le montant total des pertes déclarées au CAFC augmente depuis 2016; on pense que le nombre réel est plus élevé que celui indiqué. Dans les deux dernières années, les résidents de l'Ontario, de l'Alberta, du Québec et de la Colombie-Britannique ont signalé les pertes les plus importantes (dans cet ordre).

La fraude en valeurs mobilières ne fait pas nécessairement autant de victimes que d'autres types de fraude, mais elle fait partie des formes de fraude qui entraînent les pertes les plus importantes. Un seul stratagème de manipulation des marchés boursiers peut entraîner des pertes de plusieurs millions de dollars pour les victimes. Par exemple, trois Canadiens ont été accusées en janvier 2020 par la Securities and Exchange Commission (SEC) des États-Unis d'avoir

supposément mené un stratagème de manipulation des marchés boursiers ayant touché au moins 45 sociétés sur quatre continents et entraîné des pertes de 35 millions de dollars américains.

Neuf GCO seraient impliqués dans la fraude en valeurs mobilières (plus précisément, la manipulation des marchés), un nombre qui est resté relativement stable au cours des dernières années. Bien que ce nombre représente une petite proportion seulement des GCO recensés, les groupes impliqués représentent tous une menace élevée, ce qui semble indiquer que les groupes doivent être en mesure de mener des activités complexes et avoir un important réseau et une grande portée pour arriver à leurs fins et éviter les poursuites. Cela pourrait aussi signifier que les GCO qui se livrent à la fraude en valeurs mobilières doivent disposer de capitaux considérables pour mener à bien un stratagème de manipulation boursière.

Les stratagèmes ciblent les investisseurs du Canada et de l'étranger. Des GCO, des entreprises du secteur privé, des courtiers d'assurances et des sociétés de placement peuvent travailler ensemble pour surévaluer les investissements potentiels et camoufler des activités criminelles. Des réseaux criminels internationaux mènent des stratagèmes dans plusieurs pays. À son point culminant, le domaine des options binaires (une option financière dans laquelle le gain est soit un montant monétaire fixe, soit rien du tout) en Israël a fait des victimes au Canada, aux États-Unis, en Europe, en Afrique et au Moyen-Orient.

Définitions de fraudes en valeurs mobilières

Pump and dump – une forme de fraude dans laquelle le prix d'une action détenue est artificiellement gonflé par le biais de déclarations positives fausses et trompeuses, afin de vendre les actions achetées à bas prix à un prix plus élevé.

Stratagème d'offre initiale de pièces de monnaie – un moyen de lever des fonds sur Internet pour financer le lancement d'une nouvelle monnaie virtuelle. Les investisseurs se voient proposer des actifs numériques ou des « jetons » dont la valeur et l'utilisabilité éventuelles sont liées au succès du projet financé. Les marchés de ces actifs sont moins réglementés que ceux de capitaux traditionnels et présentent un risque accru de fraude.

Stratagème Ponzi – une forme de fraude dans laquelle la croyance en la réussite d'une entreprise inexistante est favorisée par le paiement de rendements rapides aux premiers investisseurs à partir de l'argent investi par des investisseurs ultérieurs.

Stratagème Pyramid – une forme de fraude par laquelle les membres se voient promettre un paiement ou des services pour inscrire d'autres personnes dans le système, plutôt qu'en fournissant des investissements ou en vendant des produits.

Plusieurs des GCO canadiens associés au stratagème *pump and dump* se livreraient aussi au blanchiment d'argent, probablement en utilisant leurs entreprises du secteur privé et leurs liens avec le secteur des valeurs mobilières pour blanchir les produits de leurs crimes, puisque le marché des valeurs mobilières peut offrir un rendement de 100 p. 100 ou procurer encore plus de profits, tandis que les produits blanchis par d'autres méthodes entraînent généralement des pertes.

Ces groupes entretiennent aussi des liens dans d'autres pays, surtout aux États-Unis, en Italie et en Amérique du Sud. Ces liens, qui leur permettent de faciliter d'autres activités criminelles comme l'importation de cocaïne et le trafic de drogue, peuvent sans doute être utilisés pour faire la fraude en valeurs mobilières. Afin de lutter contre la nature transnationale de cette forme de fraude et de réduire les obstacles liés aux territoires de compétence dans les enquêtes, des groupes de travail interorganismes comme l'initiative transfrontalière de lutte contre la fraude sur les marchés financiers (*Cross-Border Market Fraud Initiative* ou CBMFI) ont été formés pour détecter les activités de fraude en valeurs mobilières entre le Canada et les États-Unis.

Des criminels au Canada et à l'étranger continueront de cibler les Canadiens, étant donné le revenu moyen relativement élevé de ces derniers. Le manque de connaissances en matière de placements chez certains Canadiens continuera d'être exploité par les fraudeurs, surtout maintenant que de plus en plus de personnes utilisent Internet. Les criminels continueront d'adapter leurs activités et leurs stratégies en fonction des changements dans les moyens de communication, l'économie mondiale et les mesures de répression. Ils continueront aussi de s'adapter aux flux annuels du marché et aux tendances, par exemple en exagérant le caractère avantageux des possibilités d'investissement dans des entreprises en démarrage dans les secteurs de l'or, de l'énergie verte, de la cyberindustrie, de la médecine et du cannabis, puisque le marché boursier affiche des intérêts croissants dans ces domaines. Les offres de placement frauduleuses par Internet, surtout, continueront de prendre de l'ampleur et de représenter un risque élevé pour les investisseurs, en raison du manque généralisé de connaissances sur la légitimité et la valeur dans ce marché complexe.

FRAUDE PAR CARTE DE PAIEMENT

La fraude par carte de paiement est considérée comme une activité très payante et peu risquée. Les stratagèmes peuvent être menés avec ou sans carte. On entend par fraude sans carte une transaction frauduleuse effectuée sans la carte ni son détenteur légitime. En volant les données de la carte au moyen de technologies virtuelles (p. ex., maliciels, hameçonnage) ou de matériel (p. ex., écumoires de cartes, faux claviers d'identification personnelle), les criminels peuvent faire des achats frauduleux en ligne et en magasin.

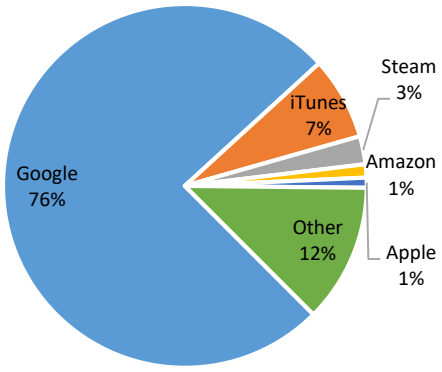
La fraude sans carte est maintenant la forme de fraude par carte de paiement la plus répandue. La technologie à puce sur les cartes a poussé les criminels à miser plutôt sur les activités en ligne, puisque la fraude sans carte, surtout les cartes de crédit et les cartes-cadeaux, peut être effectuée de façon anonyme par Internet.

Les pertes liées à la fraude par carte de crédit sont considérablement plus élevées que celles liées à la fraude par carte de débit. Dans la dernière décennie, on a observé une augmentation de 71 p. 100 du nombre de comptes de carte de crédit canadiens liés à au moins une fraude. Selon l'Association des banquiers canadiens, les institutions financières ont remboursé 862 millions de dollars à des détenteurs de cartes de crédit canadiens en 2018. Cependant, la même année, des pertes d'un peu plus de six millions de dollars canadiens (moins d'un pour cent) liées à la fraude par carte de crédit ont été signalées au CAFC. Cette tendance marquée à ne pas déclarer les fraudes aux organismes d'application de la loi entraîne des défis pour les enquêtes et le ciblage des criminels impliqués.

Vingt-deux GCO seraient impliqués dans la fraude par carte de paiement, un nombre qui est resté relativement stable au cours des cinq dernières années. Ces groupes exercent aussi des activités dans d'autres marchés criminels, comme les drogues illicites, le vol, d'autres types de fraudes et le blanchiment d'argent, et pourraient utiliser les produits obtenus par la fraude par carte de paiement pour financer leurs autres activités criminelles. Ces groupes sont surtout basés en Ontario et en Colombie-Britannique, mais compte tenu de leur capacité de cibler des victimes partout dans le monde avec Internet, ils peuvent faire de la fraude par carte de paiement à l'extérieur de leur région. De ces GCO, 82 p. 100 ont une portée interprovinciale et 50 p. 100, une portée internationale, quoique ce soit principalement pour leurs activités liées aux drogues illicites.

Les GCO utiliseront probablement de plus en plus la fraude par carte-cadeau et carte de crédit prépayée pour blanchir des produits de la criminalité, puisque cette méthode est anonyme et facilement monnayable. Dans la première moitié de 2019, des pertes de près de 700 000 $ ont été signalées par des résidents d'Edmonton (Alberta) victimes de fraude par carte-cadeau (la **figure 10** illustre la répartition des types de cartes utilisées). Les fraudeurs sont entrés en contact avec les victimes par téléphone, par courriel et par messagerie texte en utilisant des méthodes de fraude par marketing de masse comme l'hameçonnage, les stratagèmes de services du gouvernement (surtout celui de l'ARC), la piraterie d'ordinateur, la prise de contrôle de comptes, l'escroquerie du prix gagné et les stratagèmes de rencontre. Ces activités étaient menées à partir de l'Afrique, de la Malaisie, de la Turquie, du Royaume-Uni et de l'Inde, ce qui démontre la portée internationale de la fraude par carte de paiement. De plus, des cartes-cadeaux peuvent être échangées contre des bitcoins, qui peuvent ensuite être vendus pour obtenir de l'argent en différentes devises sur les sites de bureaux de change internationaux, ce qui donne aux GCO et aux criminels un autre moyen de blanchir de l'argent. (Voir la section sur la cryptomonnaie à la page 17.)

Figure 10 – Proportion de la fraude par carte-cadeau à Edmonton (de janvier à juin 2019), par entreprise



Source : Service de police d'Edmonton

Alors que la technologie évolue et que le commerce électronique prend de l'expansion, il demeurera difficile d'identifier et de cibler les criminels qui font de la fraude par carte de paiement. En raison de l'utilisation accrue du Web profond et de la création de nouveaux appareils sans fil connectés à Internet, les organismes d'application de la loi auront de

plus en plus de difficulté à identifier et à poursuivre les fraudeurs qui sévissent dans le monde virtuel, dans l'anonymat. Des organisations partout dans le monde pourraient augmenter leurs dépenses en cybersécurité en vue d'empêcher les atteintes liées aux données des cartes.

Alors que des mesures de sécurité, comme la technologie à puce sur les cartes de crédit, offrent une certaine protection contre le matériel utilisé pour la fraude par carte de paiement, l'écrémage demeurera une menace tant que les cartes à bande magnétique et le paiement sans contact seront utilisés. Compte tenu de la nature virtuelle de la fraude par carte de paiement, il sera aussi difficile d'appliquer des mesures à l'échelle mondiale pour cibler les opérations transfrontalières, car les politiques et règlements de sécurité varient d'un pays à l'autre.

FRAUDE IMMOBILIÈRE

Les stratagèmes de fraude liés à l'immobilier comprennent la *fraude pour obtenir un domicile*[5] et la *fraude visant les profits financiers*. Le deuxième type, qui peut être très lucratif pour les GCO, englobe les stratagèmes d'achat-revente, la surévaluation, la fraude hypothécaire et la fraude reliée au titre de propriété. Parmi les facilitateurs de cette activité, mentionnons le recours à des entreprises fictives et à des « acheteurs de paille »[6] afin de camoufler l'acquisition et le droit de propriété, ainsi qu'à des prêteurs fantômes (non réglementés par le système bancaire canadien) pour éviter la détection. La fraude immobilière comporte aussi souvent la collusion avec des professionnels comme des prêteurs, des agents immobiliers, des avocats et des assureurs pour faciliter la préparation, la réalisation et le camouflage de la fraude. Les GCO impliqués dans la fraude immobilière ciblent les investisseurs en immobilier, les propriétaires ou locataires de maison et les grandes banques du Canada.

Huit GCO, la plupart en Colombie-Britannique et en Alberta, se livreraient à la fraude hypothécaire, ce qui représente une légère augmentation par rapport aux années précédentes. De ces groupes, six sont aussi impliqués dans le blanchiment de produits de la criminalité, y compris le blanchiment réalisé à partir d'opérations immobilières. D'ailleurs, comme le montre le **tableau 4**, plusieurs de ces groupes possèdent une expertise en immobilier ou sont de connivence avec des professionnels dans le domaine pour réaliser leurs activités de fraude. Étant donné la tendance du crime organisé à blanchir de l'argent dans le secteur immobilier canadien, les fraudes immobilières ne cesseront pas, d'autant plus que des tactiques comme la surévaluation des propriétés et les stratagèmes d'achat-revente facilitent le blanchiment d'argent.

Tableau 4 – Exemples notables de GCO se livrant à la fraude immobilière

Recours à une entreprise fictive et à un avocat complice qui facilitent le travail administratif pour la fraude hypothécaire.
Courtier en hypothèque remplit des demandes frauduleuses et obtient des logements destinés à des fins criminelles.
Courtier en hypothèque finance des hypothèques pour des propriétés utilisées à des fins de fraude en matière d'assurance.
Ciblage des immeubles locatifs dont le propriétaire est absent et recours à un notaire complice pour faire approuver la vente frauduleuse de la propriété.
Courtier en hypothèque obtient des hypothèques à risque élevé pour les membres du groupe pour des propriétés utilisées à des fins criminelles, comme le blanchiment d'argent.

La fraude immobilière peut entraîner d'importantes pertes financières. Un stratagème mené en Alberta pendant plusieurs années a entraîné des pertes de plus de 30 millions de dollars canadiens pour la Banque de Montréal, en raison de prêts hypothécaires frauduleux créés par un groupe de criminels. La fraude en matière de titres (en utilisant des informations personnelles volées ou des documents falsifiés pour transférer le titre d'une maison à l'insu du propriétaire), quoique peu répandue au Canada, peut aussi entraîner d'importantes pertes financières, mais elle est normalement couverte par les compagnies d'assurances, qui absorbent la majeure partie des coûts liés à la fraude. L'Association canadienne des chambres d'immeuble estime que le prix moyen d'une résidence au Canada (en janvier 2020) est d'un peu plus de 500 000 $CAN, ce qui fait de la fraude en matière de titres un crime potentiellement lucratif pour ceux qui peuvent faciliter la vente frauduleuse d'une résidence.

[5] Equifax Canada a déclaré une augmentation de 52 p. 100 du nombre de signalements de fraude hypothécaire de 2013 à 2017. Cette hausse peut probablement être attribuée en grande partie à des stratagèmes de fraude en vue d'obtenir un domicile, commis par des propriétaires qui fournissent de faux renseignements dans leur demande de prêt. Ces stratagèmes sont de plus en plus répandus, étant donné les coûts à la hausse des propriétés au Canada et les normes toujours plus sévères en matière de prêts des institutions financières. Comme ce type de fraude n'est pas motivé par l'appât du gain, l'implication des GCO est minime.

[6] Un acheteur de paille est un intermédiaire qui achète quelque chose pour le compte d'une autre personne afin de contourner les restrictions légales ou permettre la fraude.

Les pertes réelles sont probablement beaucoup plus élevées que les pertes signalées. Les méthodes de dissimulation utilisées (acheteurs intermédiaires, propriété effective, prêteurs non réglementés) empêchent de comptabiliser les pertes avec précision et compliquent la détection des activités frauduleuses. De plus, le signalement des opérations douteuses au CANAFE demeure relativement faible chez les professionnels du secteur de l'immobilier. De 2013 à 2017, 2,5 millions d'opérations immobilières ont été effectuées au Canada, mais seulement 200 opérations douteuses ont été déclarées.

Les provinces où la fraude immobilière est la plus courante, comme la Colombie-Britannique et l'Ontario, sont celles où le prix moyen des maisons est le plus élevé (de 627 855 $ à 728 044 $), ce qui indique que les GCO continuent d'exercer leurs activités de fraude dans les secteurs où le potentiel de réaliser des gains est le plus élevé. Si le coût des propriétés augmente dans d'autres régions au pays, la fraude immobilière visant les profits financiers augmentera probablement aussi.

Enfin, des criminels qui se spécialisent dans le courtage hypothécaire sont susceptibles de cibler le bassin grandissant d'emprunteurs qui ne sont pas en mesure d'obtenir un prêt d'une institution réglementée et de les aider à remplir des demandes frauduleuses ou de les pousser à collaborer avec des prêteurs fantômes qui leur imposeront des taux d'intérêt gonflés. Cette tendance pourrait être de plus en plus répandue dans des villes comme Vancouver et Victoria (C.-B.) et Toronto et Hamilton (Ontario) qui, selon l'évaluation menée par la Société canadienne d'hypothèques et de logement en 2019, représentent un risque modéré concernant la surévaluation (p. ex. le coût du logement dépasse le revenu personnel).

GLOSSAIRE D'ABRÉVIATIONS ET D'ACRONYMES

Voici la liste des abréviations et acronymes utilisés dans le présent rapport.

$CAN	Dollar canadien
ARC	Agence du revenu du Canada
BATC	Blanchiment d'argent fondé sur les transactions commerciales
BMHL	Bande de motards hors-la-loi
CAFC	Centre antifraude du Canada
CANAFE	Centre d'analyse des opérations et déclarations financières du Canada
CBMFI	Cross-Border Market Fraud Initiative
DDN	Date de naissance
EIM	Évaluation intégrée des menaces
ETF	Entreprise de transfert de fonds
EUROPOL	Agence de l'Union européenne pour la coopération et la formation des services répressifs
GAFI	Groupe d'action financière international
GCO	Groupe du crime organisé
ISDE	Innovation, Sciences et Développement économique Canada
KYC	Know Your Customer
LOTA	Land Owner Transparency Act
LRPCFAT	Loi sur le recyclage des produits de la criminalité et le financement des activités terroristes
NAS	Numéro d'assurance sociale
ONUDC	Office des Nations Unies contre la drogue et le crime
PBA	Professional qui fait du blanchiment d'argent
PDG	Président-directeur général
PIB	Produit intérieur brut
PNRC	Prévision nationale du renseignement criminels
SCRC	Service canadien de renseignements criminels
SEC	Security Exchange Commission
SIM	Subscriber Identity Module
SITF	Système informel de transfert de fonds
TEF	Transfert électronique de fonds