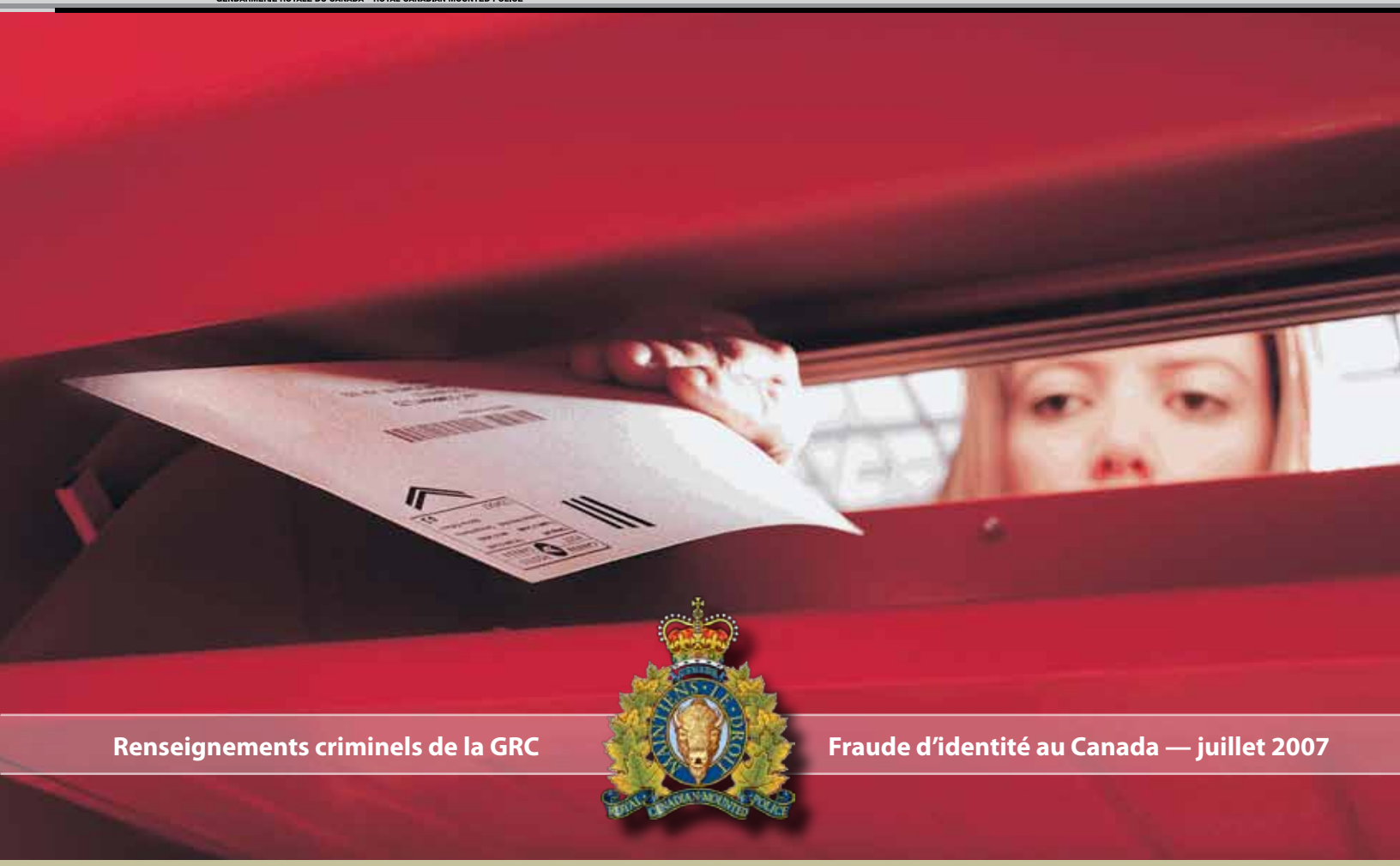
Non classifié



Renseignements criminels de la GRC

Fraude d'identité au Canada — juillet 2007

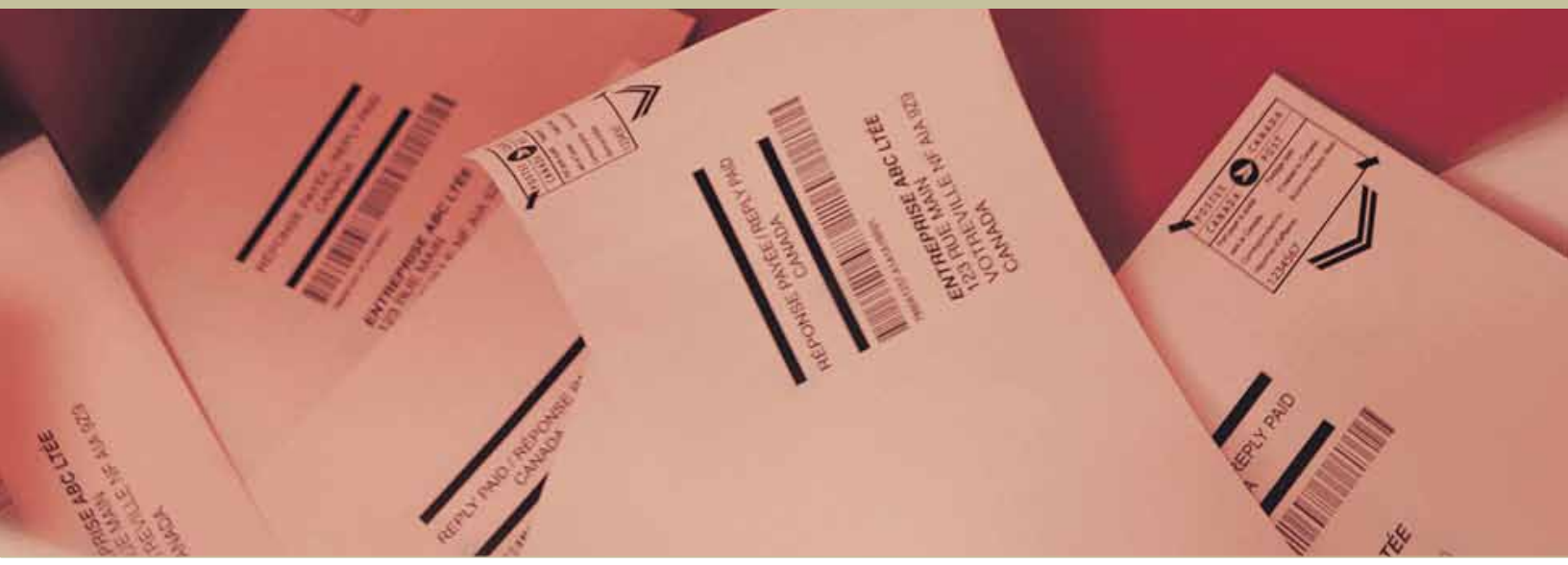


Table des matières

Table des matières

Sommaire

La fraude d'identité est une activité criminelle à faible risque et très lucrative. De ce fait, le crime organisé conventionnel et d'autres opportunistes sont de plus en plus actifs sur ce « marché ». Les renseignements personnels sont devenus un produit criminel de grande valeur; le trafic de renseignements personnels, et la fraude au moyen de renseignements personnels sans autorisation générant des profits importants pour les criminels.

La sensibilisation du public canadien à la fraude d'identité a augmenté à la suite de deux événements clés : le complot terroriste de Ahmed Ressam, ainsi que les attentats terroristes du 11 septembre aux États-Unis. Le présent rapport ne met pas l'accent sur l'activité terroriste liée à la fraude d'identité.

La majorité des cas documentés dans le présent rapport révèlent que les criminels commettent la fraude d'identité pour générer des profits financiers. Pour un grand nombre, l'un des bénéfices calculés correspond à la dissimulation de la véritable identité du criminel. Le rapport révèle également que des criminels utilisent ou achètent des fausses pièces d'identité dans le but précis de dissimuler leur identité ou leurs condamnations antérieures, de manière à faciliter des activités criminelles comme le trafic de stupéfiants et les infractions en matière d'immigration. La dissimulation de la véritable identité soulève des défis en termes d'enquêtes pour les organismes d'application de la loi.

Les criminels qui se livrent à la fraude d'identité au Canada vivent dans des régions à la fois urbaines et rurales, ciblent leurs propres quartiers, voyagent pour commettre des fraudes et ciblent des victimes internationales. Les criminels utilisent à la fois des techniques rudimentaires et des techniques extrêmement évoluées, et il s'agit autant d'individus travaillant seuls que de groupes du crime organisé. Certains coupables de fraude d'identité choisissent leurs victimes au hasard, alors que d'autres les choisissent en fonction de facteurs comme leur valeur financière, leur statut en termes de résidence, leur origine ethnique, leur vulnérabilité, ou leurs relations avec le criminel lui-même.

Parmi les près de 200 enquêtes que le présent rapport documente, de 2001 à 2006, plus de 20 employés corrompus ont été découverts. La majorité est motivée par un gain financier; toutefois, on a également constaté que les remboursements de dette et les relations personnelles étaient des facteurs de motivation.

La fraude d'identité est un crime international qui a des répercussions très personnelles. Même lorsque les victimes sont en mesure de récupérer leurs pertes financières, elles éprouvent un sentiment de violation de leur intimité et peuvent consacrer beaucoup de temps au rétablissement de leur réputation à la fois personnelle et financière. Certaines victimes canadiennes ont été arrêtées ou ont fait l'objet d'enquêtes de la police, en raison du fait que leurs renseignements personnels avaient été utilisés pour faciliter des activités criminelles.

Les victimes canadiennes vivent dans les régions tant urbaines que rurales du Canada. Elles sont ciblées par des criminels qui vivent dans le voisinage et elles sont également les victimes de stratagèmes de fraude provinciaux, nationaux et internationaux. Les victimes sont des particuliers, vivants et décédés, des entreprises et des pouvoirs publics.

Les renseignements personnels compromis servent à commettre une fraude immédiatement, ou sont mémorisés pour être utilisés à une date ultérieure et recyclés par les groupes criminels. Des Canadiens qui ont été la cible d'un vol d'identité ont été à nouveau victimes à plusieurs reprises.

Les entités des secteurs public et privé sont ciblées par les criminels pour les renseignements personnels qu'elles détiennent concernant des clients et des employés. Les entreprises hésitent souvent à signaler les violations des renseignements personnels, étant donné les possibilités de répercussions négatives, notamment la perte de confiance des consommateurs.

Le vol de courrier postal est une méthode courante, efficace et simple d'un point de vue technologique, utilisé pour acquérir des renseignements personnels sur un grand nombre de particuliers et d'entreprises.

Il existe un lien solide entre la consommation de méthamphétamine et la fraude d'identité en Colombie-Britannique et en Alberta. Au fur et à mesure que s'étend la consommation de ce stupéfiant au Canada, il est probable que le nombre des délits de fraude d'identité liés à cette consommation augmentent également.

Les documents de voyage falsifiés, modifiés et authentiques et d'autres pièces d'identité sont le nerf de la guerre pour les passeurs de migrants clandestins et l'immigration illégale en général. L'introduction clandestine de migrants et le trafic de documents pour faciliter les infractions en termes d'immigration sont des activités criminelles lucratives.

La technologie a une influence importante sur la prolifération des délits de fraude d'identité. Les coupables de fraude d'identité canadiens, du haut en bas de l'échelle, utilisent la technologie pour faciliter leurs délits. De plus, des Canadiens sont ciblés en ligne par des criminels dans le cadre de stratagèmes de fraude internationaux.

Les auteurs de fraude d'identité utilisent des entreprises de transfert de fonds ou de vente de titres négociables (entreprises de services monétaires) pour percevoir l'argent des cibles de leur fraude, échanger de l'argent contre des données avec d'autres criminels et transférer à l'étranger des revenus illicites. Les profits réalisés vont de petites sommes à des millions de dollars et, dans ce dernier cas, les produits de la fraude ne sont parfois jamais récupérés.

La violence est une menace émergente associée aux délits de vol d'identité. Au fur et à mesure que les délits de fraude d'identité deviennent plus lucratifs, ils attirent des groupes ou des particuliers impliqués dans des crimes violents.

Les délits de fraude d'identité ont évolué. À l'heure actuelle, les infractions au *Code criminel* ne traitent pas adéquatement les activités associées à l'acquisition, à la possession ou au commerce illicites de renseignements personnels dans l'intention de commettre un délit (les données de cartes de paiement et les passeports constituent l'exception).

Les stratégies d'éducation et de sensibilisation donnent à la population les outils requis pour détecter et prévenir les stratagèmes de fraude, qui évoluent constamment. Toutefois, elles ne traitent ni n'abolissent la responsabilité des institutions des secteurs public et privé de faire preuve de diligence raisonnable en matière de renseignements personnels et de compromission de cette information.

Introduction

Le présent rapport est un projet national d'évaluation du renseignement stratégique sur la fraude d'identité au Canada. Il documente des enquêtes canadiennes sur des fraudes d'identité, afin de déterminer l'ampleur du problème au Canada et d'évaluer les tendances émergentes et existantes en termes de fraude d'identité.

La Sous-direction des délits commerciaux (SDDC) de la GRC a commandé cette évaluation stratégique en raison de la limitation de la documentation et de l'analyse nationales des enquêtes sur les vols d'identité de la police canadienne.[1]

La SDDC de la GRC définit comme suit la fraude d'identité :

> *La fraude d'identité [comprend] l'acquisition, la possession ou le commerce illicite de renseignements personnels et l'utilisation non autorisée de ces renseignements dans le but de créer une identité fictive ou d'emprunter une identité existante ou d'en prendre le contrôle afin d'obtenir des profits financiers, des biens ou des services ou de dissimuler des activités criminelles.*

Les enquêtes ont été soumises par la GRC et par les services de police provinciaux et municipaux de 2001 à aujourd'hui. L'ensemble de ces dossiers doit être considéré comme un aperçu de la fraude d'identité au Canada, étant donné qu'on estime que chaque année, des centaines d'enquêtes canadiennes sur l'application de la loi comportent un volet fraude d'identité.

La présente évaluation n'inclut pas la fraude visant les cartes de paiement en tant que fraude d'identité, sauf lorsque des renseignements personnels ont été compromis en plus des numéros de carte de crédit ou de débit.

De l'information a été réunie essentiellement sur les criminels qui se livrent à l'acquisition, à la possession ou au commerce de renseignements personnels à des fins de fraude d'identité, à la fabrication de pièces d'identité frauduleuses ou à l'utilisation de renseignements personnels ou de pièces d'identité contrefaites pour commettre des fraudes. Elle fait le lien entre ces criminels et le crime organisé qui est impliqué dans d'autres délits criminels, notamment le trafic de stupéfiants ou les infractions en matière d'immigration, le cas échéant.

Les termes *vol d'identité* et *fraude d'identité* sont souvent utilisés indistinctement. La Sous-direction des délits commerciaux de la GRC utilise le terme fraude d'identité pour deux raisons. D'abord, il n'existe aucun délit adéquat prévu par le *Code criminel* pour couvrir l'acquisition, la possession ou le commerce illicites de renseignements personnels dans le but de commettre un délit, c'est-à-dire l'aspect « vol » de l'acte criminel. Ensuite, la grande majorité des délits commis en utilisant des renseignements personnels sans autorisation comportent un volet frauduleux.

L'expert en sécurité de haute technologie Bruce Schneier soutient que le terme « vol d'identité » est trompeur. Il dit : « L'identité n'est pas une possession qui peut être acquise ou perdue [...] [L]e crime réel dans ce cas est la fraude, plus précisément, l'usurpation d'identité en vue de commettre une fraude [...] [I]l n'y a aucunement vol d'identité; plutôt, les renseignements d'identification sont utilisés de manière malveillante pour commettre une fraude. »[3]

Exemples de méthodes utilisées pour acquérir des renseignements personnels :	Exemples de fraudes commises en utilisant des renseignements personnels sans autorisation :
Corruption d'employés	Fraude visant des cartes de paiement
Marketing de masse frauduleux	Fraude visant des chèques
Vol (courrier, portefeuille)	Fraude visant des hypothèques et titres de propriété
Introduction par effraction dans des résidences, des véhicules et des entreprises	Fraude visant des assurances
Fouille de poubelles*[2]	Fraude visant des programmes, des services et des prestations du gouvernement
Hameçonnage*, Pharming* (empoisonnement du système de nom de domaine), logiciels espions*	Fraude visant des documents du gouvernement
Accès non autorisé à un ordinateur	Fraude en matière d'immigration
Méfait concernant des données	Fraude bancaire (comptes frauduleux, prises de contrôle de comptes, prêts)
Sources ouvertes sur Internet	Fraude visant un compte (téléphones cellulaires)
Exploitation des modes de socialisation à des fins d'escroquerie (ingénierie sociale)*	Fraude électorale

1 Pour un vaste portrait stratégique du vol d'identité au Canada, l'auteur recommande la lecture du rapport sur le vol d'identité : Rapport présenté à la ministre de la Sécurité publique et de la Protection civile du Canada et à l'Attorney General des États-Unis, Groupe de travail binational sur les fraudes transfrontalières par marketing de masse, octobre 2004. http://www.securitepublique.gc.ca/prg/le/bs/report-fr.asp

2 * Voir annexe B — Glossaire de tous les termes identifiés par un astérisque.

3 Bruce Schneier, Solving Identity Theft, Forbes.com, Security Matters, 22 janvier 2007.

Auteurs de fraude d'identité au Canada

Les criminels reconnaissent que les renseignements personnels sont un bien criminel précieux. Le crime organisé (CO) « conventionnel » accorde donc de plus en plus d'intérêt à la fraude d'identité en tant qu'entreprise criminelle, non seulement pour utiliser des pièces d'identité et des pseudonymes frauduleux pour dissimuler sa véritable identité, mais également pour faciliter ses activités criminelles.

D'autres groupes criminels, comme les gangs de rue et les voleurs de courrier dans le Lower Mainland de la C.-B. ont un grave impact sur les individus, les collectivités et les entreprises. De plus, un grand nombre de complots complexes sont dirigés par des individus qui ont de vagues liens avec d'autres criminels, mais qui ne constituent pas en eux-mêmes une organisation criminelle.

Les enquêteurs remarquent que même le plus rudimentaire des criminels maîtrise l'informatique. Un grand nombre ont des ordinateurs portables avec des modèles pour de nombreux types de pièces d'identité de provinces multiples. Sur leurs ordinateurs, ils stockent également les profils de renseignements complets sur de nombreuses cibles. L'absence de « sophistication » de ces criminels confirme le fait que les renseignements personnels des Canadiens, où qu'ils se situent, sont faciles à obtenir.

Les techniques non raffinées sont également efficaces. Nombre d'enquêtes à l'échelle du pays ont révélé que les criminels inscrivaient les profils personnels sur papier ou dans des carnets de notes qui sont faciles à transporter et ne laissent aucune trace électronique. Parfois, des méthodes à faible et à haut niveau technologique sont utilisées simultanément. Par exemple, les groupes réunissent des renseignements personnels sur des cibles au moyen à la fois de vol de courrier et de piratage informatique ou les individus qui mémorisent des profils personnels dans des carnets de notes fabriquent des pièces d'identité frauduleuses au moyen d'ordinateurs, de logiciels et d'autres équipements.

Crime organisé

Le CO dissimule l'activité criminelle sous les apparences d'une pratique commerciale normale. L'utilisation d'identité fictive ou obtenue de manière frauduleuse pour enregistrer des téléphones cellulaires, des entreprises, acheter des propriétés, louer des véhicules, dissimuler des casiers judiciaires ou franchir des frontières est bien documentée.

Nombre de groupes criminels au Canada se livrent à la fraude d'identité. Cela inclut, de manière non exclusive, le CO basé en Asie, les réseaux criminels d'Afrique de l'Ouest et de l'Est, les groupes criminels basés au Sri Lanka, au Pakistan ou au Moyen-Orient et les gangs de rue. Tout comme le CO en général, nombre de groupes criminels qui se livrent à la fraude d'identité ne peuvent être qualifiés en termes d'origine ethnique.

Opportunistes

Certains opportunistes cités dans le présent rapport ont tiré des profits importants de leurs activités de fraude d'identité. Même s'il est difficile de classifier les opportunistes coupables de fraude d'identité, certains se constituent un créneau en fournissant des services, comme la fabrication de documents ou la fourniture d'informations. D'autres criminels commettent des fraudes d'identité essentiellement pour des gains financiers personnels.

Certains des coupables de fraude d'identité les plus avertis sont des individus et non des organisations. Ils illustrent également combien il est facile pour une personne de faire l'acquisition de milliers de renseignements personnels et de frauder un grand nombre d'individus, d'organisations et d'organismes gouvernementaux. En termes de fraude d'identité, les individus peuvent être aussi dangereux que les organisations criminelles.

Activités criminelles multiples

Les coupables de fraude d'identité ont des antécédents criminels qui incluent la fraude, la falsification de documents, les enchères frauduleuses sur Internet, les fraudes en matière d'investissement, la contrefaçon de billets de banque et de cartes de crédit, la fraude au moyen de chèques, la fraude par tirage à découvert*, l'hameçonnage* et la fraude de guichet automatique de banque (GAB). Des renseignements anecdotiques ont permis de déterminer que les faux monnayeurs se livrent à la fabrication de fausses pièces d'identité. Les coupables de fraude d'identité participent à de nombreuses autres activités criminelles non liées à la fraude.

Trafic de stupéfiants

Il existe un lien entre la consommation de méthamphétamine ou la dépendance à l'égard de cette substance et les crimes de fraude d'identité, qui est traité en détail plus loin dans cette section. D'autre part, un certain nombre de cas ont révélé des liens avec les stupéfiants. Cela inclut à la fois le trafic de stupéfiants par des coupables de fraude d'identité et des individus qui opèrent en utilisant des pseudonymes et des fausses identités.

Les médias ont relaté qu'un courtier hypothécaire de Vancouver travaillait en collusion avec des agents immobiliers, pour faire l'acquisition frauduleuse de maisons qui servaient ensuite de serre de culture de marihuana. On a relaté que le courtier et les complices avaient des lettres d'emploi falsifiées pour les acheteurs. On pense que les noms utilisés pour les demandes d'hypothèque étaient des nouveaux immigrants de la communauté vietnamienne qui n'avaient aucune connaissance du stratagème.

Certaines lettres d'emploi incluaient les numéros résidentiels des courtiers ou de l'agent immobilier impliqués. Dans certaines transactions immobilières, les enquêteurs n'ont pas été en mesure de vérifier la source d'acomptes importants, parfois de plus de 100 000 $.[4]

Ce cas semble indiquer que les criminels pourraient avoir blanchi des revenus tirés d'activités criminelles pour verser des acomptes sur l'achat de maisons qui servaient ensuite à faire pousser de la marihuana. Les identités des criminels étaient protégées, parce qu'ils n'étaient pas répertoriés comme propriétaires du bien. Lorsqu'ils vendaient à un moment donné les résidences, ils réalisaient un profit supplémentaire sur la propriété.

4 Kim Bolan, « 100 grow-op houses found in mortgage scam probe », Vancouver Sun, 25 septembre 2004, p. A1.

Vol de courrier et fraude d'identité dans le Lower Mainland de la C.-B.

Une sous-culture de voleurs de courrier et de coupables de fraude d'identité a fait son apparition dans le Lower Mainland de la C.-B. au cours des cinq dernières années. Ce phénomène mérite d'être décrit en détail, en raison de ses sérieuses conséquences sur les individus, les collectivités et les entreprises de cette région.

Le vol de courrier est un crime très efficace et nécessitant peu de technologies, qui sert à faire l'acquisition de renseignements personnels pour commettre de la fraude d'identité. Les criminels du Lower Mainland de la C.-B. sont devenus de plus en plus raffinés, organisés et leur modus operandi (M.O.) ne cesse d'évoluer.

Méthamphétamine et fraude d'identité

Santé Canada déclare que la consommation de méthamphétamine au Canada a augmenté au cours des dernières années, particulièrement dans l'Ouest canadien.[5] Cela confirme le résultat des enquêtes de la Colombie-Britannique, de l'Alberta et du Manitoba, qui font le lien entre la consommation de méthamphétamine et la fraude d'identité.

Les voleurs de courrier dans le Lower Mainland de la C.-B. sont des consommateurs ou dépendants de la crystal meth. Une partie des effets de ce stimulant, comme l'état de veille, l'augmentation de la résistance et de la vigilance, ainsi que le « high » prolongé de 4 à 12 heures[6] favorisent la réalisation des tâches prolongées répétitives d'introduction par effraction dans les boîtes aux lettres, de tri du courrier et de création de profils d'identité, de fouille de poubelles* et d'essai de cartes de crédit en ligne, pour vérifier si elles sont actives.

Les services de police dans l'Ouest canadien ont décelé un lien entre la consommation de méthamphétamine et l'augmentation de la criminalité dans la région, notamment le vol d'automobiles, les armes, la fraude d'identité et la fraude.

Ce cas démontre la vivacité, le savoir-faire technologique, la portée internationale et l'évolution des délits commis par ce réseau de fraude d'identité et de méthamphétamine. Il révèle combien il est facile d'acquérir des renseignements personnels, tant à l'échelon local qu'international. Comme c'est le cas pour un nombre important de coupables de fraude d'identité, les membres de ce groupe ne cessaient de récidiver.

Le *Rapport sur la situation des stupéfiants illicites au Canada de 2005 de la GRC* recense des indices d'une augmentation de la production de méthamphétamine au Canada :

> L'implication du crime organisé dans le commerce de la méthamphétamine s'est traduite par l'augmentation du nombre des « super » laboratoires de méthamphétamine;

> L'expansion vers l'Est de la production et de la distribution de méthamphétamine s'est poursuivie en 2005. En fait, le nombre de sites de production de la méthamphétamine en Ontario n'a été dépassé que par celui des sites de la Colombie-Britannique.

On craint qu'au fur et à mesure que la production et la consommation de méthamphétamine s'étendent à l'échelle du Canada, les délits de fraude d'identité associés à la consommation de méthamphétamine ou à la dépendance qu'elle entraîne augmentent également.

5 Site Web de Santé Canada, « Soit plus futé que les stupéfiants, les faits : méthamphétamine », http://drugwise-droguesoisfute.hc-sc.gc.ca/facts-faits/meth_e.asp

6 Ibid.

Fraude d'identité et trafic de méthamphétamine

Un article de USA Today relate l'histoire d'un réseau de fraude d'identité d'Edmonton, qui a beaucoup exploité le stratagème de la fouille de poubelles* derrière les banques, les points de vente au détail, les entreprises de télécommunications, les agences de location automobile, les restaurants et les magasins de location de vidéos, et les résidences de particuliers pour trouver des renseignements personnels et créer des profils personnels. L'article rapporte que le réseau de fraude trouvait des données comme des transactions par carte de crédit, des demandes de prêt, des rapports de services à la clientèle, des manuels d'employé, des répertoires téléphoniques internes, des profils de crédit d'agences de rapports de crédit, des dates de naissance et des adresses.

Le groupe maîtrisait l'informatique et utilisait les services de téléphone par voix sur IP (VoIP), qui permettent à l'utilisateur de choisir n'importe quel code régional, et ainsi, de dissimuler l'emplacement où il se trouve.

Le groupe est ensuite passé à l'achat et à la vente de renseignements personnels en ligne sur les réseaux de service de bavardage Internet à des groupes criminels du Québec, de Roumanie, d'Autriche et d'Égypte, auxquels il achetait des profils d'identité de victimes américaines. Selon l'article, le groupe d'Edmonton versait 200 $US pour un profil qui incluait un mot de passe de compte bancaire, un numéro de carte de crédit avec code de sécurité et un numéro de sécurité sociale, puis il ciblait ces victimes. Le groupe d'Edmonton versait aux autres groupes criminels de l'argent « propre », de l'argent retiré dans des GAB qui était ensuite viré au groupe criminel qui avait fourni le profil. Le groupe d'Edmonton fabriquait également ses fausses pièces d'identité en utilisant des ordinateurs, des logiciels d'édition électronique et des modèles de pièces d'identité. Il effectuait des essais sur des sites Web financiers et les exploitait, pour, par exemple, effectuer des transferts d'argent par courriel, un service offert par certaines banques canadiennes.[7]

7 Byron Acohido et Jon Swartz, « Meth addicts' other habit: Online theft », *USA Today*, 15 décembre 2005..

Infractions en matière d'immigration

Les documents de voyage et autres pièces d'identité falsifiés, modifiés et authentiques sont le nerf de la guerre pour les passeurs de migrants clandestins et la migration illégale en général. L'implication du crime organisé dans l'introduction clandestine de migrants et la fabrication de fausses pièces d'identité à des fins d'immigration illégale est bien documentée à l'échelle internationale.

Les délits de fraude d'identité associés aux délits en matière d'immigration continueront à augmenter, étant donné que le Canada est une destination de choix pour les immigrants à la recherche d'une meilleure qualité de vie. De plus, le passage clandestin de migrants et le trafic de documents pour faciliter les délits en matière d'immigration sont des activités criminelles lucratives.

Affidavit contrefait

Produits de la criminalité

La majorité des coupables de fraude d'identité évalués dans le cadre de la présente étude sont motivés par un gain financier. Les profits vont de sommes modestes à des millions de dollars, obtenus au moyen de stratagèmes dont les produits ne sont, dans certains cas, jamais récupérés. Dans de nombreux cas, en particulier ceux qui font l'objet d'une enquête pour vol de renseignements personnels, on ignore les pertes financières.

Dans les cas où le gain financier est l'objectif, la fraude par carte de paiement (essentiellement fraude par carte de crédit) est documentée plus que tout autre type de fraude. La fraude de compte bancaire est également fréquemment signalée. Par comparaison, un nombre beaucoup plus faible de fraudes hypothécaires est signalé; toutefois, ce type de fraude génère beaucoup plus de revenus (plus de 100 000 $) en une seule transaction.

Entreprises de transfert de fonds ou de vente de titres négociables (entreprises de service monétaire)

Les criminels utilisent fréquemment des entreprises de service monétaire pour soutirer de l'argent à des cibles de fraude, au moyen de stratagèmes de marketing de masse frauduleux. Ce M.O. est signalé dans le cadre de la plupart des cas de marketing de masse soumis dans le cadre de la présente évaluation.

Les coupables de fraude d'identité échangent ou acquièrent activement des renseignements personnels sur Internet. Souvent, les profits tirés de l'échange de renseignements personnels sont partagés entre toutes les parties en cause. Les entreprises de service monétaire sont utilisées pour une partie de ces transactions financières.

Le ciblage des produits de la criminalité dans les cas de fraude d'identité pourrait être un solide facteur de dissuasion pour ces criminels. Cette opinion est appuyée par un certain nombre d'enquêteurs sur les fraudes d'identité qui ont participé à l'évaluation.

TECHNOLOGIE

Le Canada est l'un des pays les plus branchés sur Internet au monde, avec une population qui a une grande maîtrise de la technologie. Les criminels canadiens sont experts en technologie et ils tirent profit de l'infrastructure Internet du Canada pour faciliter la fraude d'identité. Les criminels internationaux tirent profit de cette infrastructure pour cibler les Canadiens en vue de commettre de la fraude d'identité. Certains des stratagèmes énoncés ci-dessous sont extrêmement évolués, alors que d'autres sont simples, et pourtant efficaces.

Les pirates informatiques sont des criminels motivés par le profit. Cela démontre également que les enquêtes internationales sur les crimes informatiques sont complexes, font appel aux organismes d'application de la loi de multiples administrations et le tout avec un degré de réussite variable.

Internet et fraude d'identité

Internet est l'hôte de nombreux forums Web consacrés à la fraude d'identité. De plus en plus, les renseignements personnels sont échangés et vendus en ligne sur des sites Web restreints, par voie de messagerie instantanée et dans des salons de clavardage. L'enquête suivante fournit un exemple de la portée de l'activité criminelle sur les sites Web de fraudeurs de cartes bancaires (cardeurs)*.

Internet facilite la fraude d'identité. Les criminels ont tous accès à d'énormes volumes de renseignements personnels provenant de sources légitimes, ou du commerce criminel en ligne de données. Internet facilite l'anonymat des criminels, ainsi que la capacité de se faire passer pour légitime, comme le démontre les cas d'hameçonnage. Internet fournit également aux criminels un accès à des centaines ou des milliers de victimes potentielles par voie d'escroquerie ou d'hameçonnage.

La technologie complique les enquêtes. Les enquêtes qui portent sur Internet ou des données électroniques nécessitent une analyse judiciaire diligente des ordinateurs et d'autres dispositifs. Souvent, la preuve potentielle ne peut être extraite. Un grand nombre d'enquêtes finissent par faire appel à des compétences multiples et souvent, plusieurs États.

Opération FIREWALL[8, 9]

En 2004, une enquête internationale menée par les États-Unis a permis d'identifier trois « groupes criminels informatique clandestins » : Shadowcrew, Carderplanet et Darkprofits. Les groupes exploitaient des sites Web utilisés pour trafiquer des cartes de crédit contrefaites et de faux renseignements et documents d'identification. Ces sites Web échangeaient de l'information sur les méthodes utilisées pour commettre des fraudes, et ils fournissaient également une tribune pour promouvoir et faciliter le vol électronique des renseignements d'identification personnels, la fraude par cartes de crédit et la production et la vente de fausses pièces d'identité.

Trois individus, deux des États-Unis et l'autre de Russie, administraient le site Web Shadowcrew, en contrôlant l'identité des personnes qui devenaient membres et des animateurs. Selon l'acte d'accusation, les trois étaient responsables de l'ensemble du marché de Shadowcrew.

Après être entrés en contact initialement sur Internet, les suspects ont échangé de l'information volée et des pièces d'identité contrefaites, comme des cartes de crédit, des permis de conduire, des passeports nationaux et étrangers et des certificats de naissance. Le site Web avait près de 4 000 membres.

Dans huit États américains et six pays étrangers, 28 personnes ont été arrêtées. On estime que le groupe a fait le trafic de 1,7 million de numéros de cartes de crédit volées et les pertes des institutions financières se sont chiffrées à plus de 4,3 millions de dollars.

8 Comité de presse du Service secret des É.-U., GPA-23-04, « U.S. Secret Service's Operation Firewall Nets 28 Arrests; International Undercover Investigation Prevents Millions in Financial Loss », 28 octobre 2004.

9 Département de la justice américain, « Nineteen Individuals Indicted in Internet 'Carding' Conspiracy; Shadowcrew Organization Called One-Stop Online Marketplace for Identity Theft », 28 octobre 2004.

VICTIMES

La population est la véritable victime de la fraude d'identité. Les renseignements personnels que recherchent les criminels sont à la fois aléatoires, dans le cas des vols corporatifs d'envergure, et ciblés sur des collectivités précises, des personnes aisées, des membres de familles et des personnes vulnérables comme les jeunes, ceux qui ont besoin d'argent ou ceux qui ont des incapacités mentales.

La plupart du temps, les victimes découvrent que leurs renseignements personnels ont été violés à la suite d'une fraude. Par exemple, ils reçoivent des factures de produits et de services dont ils n'ont pas fait l'acquisition, des appels téléphoniques en rapport avec des demandes de crédit, ils se voient refuser un crédit, ils découvrent que leurs comptes bancaires sont vides, ils font une demande de passeport alors qu'un exemplaire a déjà été délivré à une autre personne en leur nom ou ils reçoivent des avis de paiements exigibles sur des hypothèques pour des maisons qu'ils possèdent depuis des années.

La plupart des victimes doivent elles-mêmes rétablir leur réputation financière. Il s'agit d'un long processus décourageant qui entraîne souvent des différends avec les institutions, et ce, avec un succès limité. Certains services de police enquêtant sur des preuves d'identité ont aidé des victimes à composer avec des institutions non coopératives.

Les institutions financières remboursent les particuliers qui sont victimes de fraude par carte de paiement et de prise de contrôle de compte. Il est fréquent que ces institutions ne considèrent pas les individus remboursés comme de véritables victimes, étant donné que leurs pertes sont indemnisées financièrement. De plus, on déclare rarement aux individus où et comment une violation a eu lieu en raison de l'enquête en cours dans l'institution. La rétention de cette information peut contribuer au sentiment d'indignation et de violation de l'intimité de la victime.

Pour les victimes, les pertes ne sont pas juste monétaires, mais personnelles. Parallèlement au sentiment d'être aliénées ou violées, les victimes peuvent ressentir de la peur, du désespoir et du harcèlement. De plus, les personnes dont les antécédents en matière de crédit sont entachés à la suite d'une fraude d'identité peuvent se voir refuser un emploi ou des autorisations de sécurité.

Une fois qu'une personne a été la cible d'une fraude d'identité, elle peut être à nouveau victimisée à de nombreuses reprises. Aussi, il est important que les individus avertissent tous les organismes pertinents, dont les bureaux de crédit. Il est crucial que les victimes fassent un rapport à la police après toute fraude commise en leur nom pour créer un dossier officiel afin de se protéger. Des victimes de fraude d'identité ont fait l'objet d'enquêtes et ont été arrêtées au Canada après des crimes commis en leur nom.

Jeunes

Les jeunes sont considérés comme un groupe émergent qui deviendra de plus en plus la cible de fraudes d'identité. Cela en raison de dossiers de crédit vierges, de la prolifération des renseignements disponibles sur Internet et de la possession par les jeunes d'un nombre croissant de documents de sécurité.

Internet

Les jeunes sont des utilisateurs prolifiques de salons de clavardage, de la messagerie instantanée et, plus récemment des sites de réseautage social. Les sites de réseautage social comme MySpace, Friendster et Facebook sont des communautés virtuelles, au sein desquelles les individus se constituent des profils personnels en affichant des photographies, des renseignements personnels, en faisant le lien avec leur profil et d'autres profils, de manière à se constituer un réseau d'amis et ensuite faire des envois multiples aux sites de leurs amis. La portée des renseignements qu'ils affichent peut être aussi limitée ou aussi vaste qu'ils le choisissent. « Nous devons partir du principe que (les réseaux sociaux) sont là pour rester. Nous devons également partir du principe qu'ils sont utiles socialement, agréables et qu'ils ont des avantages. »[10]

Du point de vue de l'application de la loi, l'affichage de renseignements personnels sur Internet accroît le risque de leurre par des prédateurs d'enfants. Combinée aux renseignements disponibles sur les jeunes provenant d'autres sources en ligne, la fraude d'identité devrait soulever des inquiétudes supplémentaires.

Documents de sécurité canadiens

Les enfants sont également vulnérables aux fraudes d'identité, étant donné qu'ils possèdent de multiples documents de sécurité canadiens à un âge précoce. Par exemple, pour bénéficier de programmes d'avantages canadiens comme le Régime enregistré d'épargne-études, les enfants ont besoin d'un numéro d'assurance sociale. Depuis 2004, les enfants canadiens ont besoin de leur propre passeport pour voyager à l'étranger. Avant 2004, les noms d'enfants mineurs pouvaient être insérés sur une étiquette de remarque apposée sur les pages du visa des passeports de leurs parents. La nouvelle politique est en vigueur pour lutter contre la traite des enfants.[11] Même si la délivrance de pièces d'identité gouvernementales aux enfants prévient certains types de fraude et d'autres crimes graves visant les enfants, de manière ironique, la possession de multiples pièces d'identité gouvernementales accroît la vulnérabilité des enfants à la fraude d'identité, étant donné que leurs renseignements personnels sont stockés à un plus grand nombre d'emplacements physiques électroniques.

10 Parry Aftab, directeur exécutif WiredSafety.org, Shannon Proudfoot, « Taking back MySpace », The Ottawa Citizen, 11 mai 2006.

11 http://www.pasportcanada.ca/ombudsman/omb-ar2005-06.aspx?lang=f

Portée géographique

La fraude d'identité est un crime international qui a des répercussions très personnelles. Nombre de crimes sont commis localement et ils ont des répercussions négatives importantes sur la collectivité locale qu'ils ciblent. Fait intéressant, la majorité des cas cités dans la présente évaluation avaient des connections dans plusieurs provinces ou des connections internationales.

Municipalités rurales

La fraude d'identité n'est pas un phénomène urbain. Certains auteurs de fraude d'identité, en fait, ciblent des petites collectivités où ils croient pouvoir éviter d'être repérés.

Dans un certain nombre de cas, on a signalé des victimes dans de petites collectivités dont les renseignements personnels avaient été utilisés dans de grands centres urbains, souvent dans d'autres provinces. Peu de victimes connaissaient la source de compromission de leurs renseignements personnels.

Scène nationale

Nombre de victimes de fraude d'identité résident dans une province différente de celle du crime ou de son auteur. Les victimes découvrent que leurs renseignements personnels ont été utilisés dans d'autres provinces pour fabriquer des pièces d'identité, acquérir des services (téléphone cellulaire ou autres), en leur soutirant de l'argent à partir de leurs comptes bancaires, au moyen de cartes de crédit et de réacheminement du courrier. Ils découvrent la compromission lorsqu'ils reçoivent des appels téléphoniques, des factures de service, des comptes d'accès ou lorsqu'ils tentent d'obtenir des services ou des documents de sécurité canadiens.

Les suspects qui résident dans une province voyagent intentionnellement dans des provinces distinctes et multiples pour commettre de la fraude. Ils ont fréquemment des antécédents d'activités criminelles dans leur province de résidence et, donc, ils commettent de la fraude dans d'autres provinces pour minimiser les risques d'être détectés ou les peines encourues.

Scène internationale

Nombre d'enquêtes sur des fraudes d'identité citées dans l'ensemble du rapport ont un lien international, qu'il s'agisse d'associés criminels, de cibles, de technologie ou d'immigration.

Les auteurs de fraude canadiens ciblent des victimes dans d'autres pays. Un certain nombre d'enquêtes ont porté sur du marketing de masse frauduleux (loterie frauduleuse, stratagème de prêt avec frais payables d'avance, fraude sur rabais gouvernementaux, stratagèmes de prêt) qui cible essentiellement des citoyens américains. On demande aux victimes d'encaisser des chèques (chèques volés légitimes qui ont été contrefaits) ou fausses traites bancaires, de garder une partie de la somme encaissée et de virer le solde aux fraudeurs. Lorsque les chèques reviennent impayés, les victimes sont responsables des montants. Dans un grand nombre de ces cas, les artistes de la fraude demandent des renseignements personnels qu'ils obtiennent des victimes, dont l'information des comptes bancaires, que les fraudeurs utilisent par la suite pour retirer des fonds dans les comptes bancaires de ces victimes.

Les Canadiens sont la cible de stratagèmes de marketing de masse frauduleux de criminels internationaux.

Les fraudes d'identité n'ont pas de frontières. Les Canadiens qui vivent dans les municipalités rurales sont aussi vulnérables aux stratagèmes de fraude d'identité que les résidents des grands centres urbains. Ils sont ciblés par les criminels actifs à l'échelon local, dans l'ensemble du Canada et sur la scène internationale. Cela est facilité par le fait que les renseignements personnels de tous les individus sont mémorisés dans des bases de données publiques et privées, qui peuvent être violées dans l'ensemble du Canada. De plus, notre infrastructure Internet signifie que les coupables de fraudes d'identité qui résident au Canada ou à l'extérieur peuvent cibler n'importe qui par Internet, peu importe le lieu de résidence.

Fraude d'identité dans les secteurs public et privé

Les institutions des secteurs public et privé sont de plus en plus ciblées par les auteurs de fraudes d'identité pour leurs données sur les clients et les employés. Le présent rapport révèle également qu'elles ne font pas preuve de la diligence raisonnable requise pour se protéger et protéger les renseignements personnels des clients contre cette menace.

Ciblage des secteurs public et privé

Les entreprises canadiennes et les institutions des secteurs public et privé sont ciblées par les auteurs de fraude d'identité, pour le vol de renseignements personnels des employés et des clients, ainsi que d'équipements et de documents vierges. Les criminels sont à la fois internes et externes. Les violations sont commises par des employés corrompus, par voie de vol électronique de données et de vol physique des données.

Les violations de l'information personnelle concernent autant les petites entreprises, avec la violation des renseignements de quelques employés ou clients, que les grandes institutions, les violations touchant des milliers de clients. Les répercussions d'une petite violation des données d'un client dans une petite entreprise peuvent être aussi dévastatrices pour les activités et la réputation d'une entreprise qu'une violation d'envergure dans une grande entreprise ou institution publique.

Étant donné que la plupart des coupables de fraude d'identité sont motivés par le gain financier, naturellement, les institutions financières sont les principales victimes corporatives de la fraude d'identité. Elles sont ciblées à la fois pour les renseignements sur leurs clients et pour leur argent dans le cadre de stratagèmes de prêt, de fraudes par cartes de paiement, de fraudes visant les comptes bancaires et de fraudes hypothécaires.

Fraude par carte de paiement

La fraude par carte de paiement (essentiellement fraude par carte de crédit) est commise plus que tout autre type de fraude liée au vol d'identité. Cela inclut les demandes frauduleuses, l'utilisation de cartes de crédit et la fabrication de fausses cartes de paiement. Dans ces cas, les cartes de paiement étaient liées à la fraude d'identité d'une façon ou d'une autre.

Les criminels reconnaissent que la fraude par carte de crédit est lucrative et facile à commettre. Les numéros de carte de crédit sont faciles à obtenir par le vol de courrier, l'écrémage ou sur les sites de fraude de cartes bancaires en ligne (cardeurs)*. Les demandes sont facilement acceptées par les institutions financières et les commerçants, que ce soit en personne ou en ligne, et demandent rarement une pièce d'identité à l'appui ou effectuent rarement d'autres vérifications de sécurité.

Fraude par chèque

Certains services de police ont constaté une prolifération récente de la fraude par chèque. Les entreprises sont victimisées par des criminels qui volent et falsifient des chèques corporatifs ainsi que des en-têtes de lettres de sociétés qui sont utilisés dans de nombreux stratagèmes criminels de marketing de masse ou autres. Les chèques légitimes sont principalement obtenus par voie de vol de courrier. L'examen manuel et physique est nécessaire pour contrer les techniques de falsification. La qualité des chèques s'améliore et ils sont souvent de qualité supérieure à la norme de retenue de cinq à dix jours.

Des faux chèques d'entreprise ont également été trouvés dans des laboratoires qui falsifient également des pièces d'identité. Des chèques d'entreprise lus optiquement ont été trouvés sur les ordinateurs de coupables de fraude d'identité.

Vol d'équipement et de documents vierges

Les pièces d'identité vierges et les équipements utilisés pour fabriquer ces pièces sont des biens précieux pour les auteurs de fraude d'identité. Les entreprises et institutions qui les possèdent doivent les manipuler et les entreposer comme s'il s'agissait d'un bien précieux.

Les coupables de fraude d'identité ont ciblé des hôpitaux pour voler des appareils à embosser les cartes, qui sont utilisés pour fabriquer de fausses pièces d'identité.

En 2005, une agence d'assurance de Stonewall au Manitoba, a été la victime d'une entrée par effraction « professionnelle », selon les représentants de la GRC interviewés par les médias. Les voleurs ont volé le matériel informatique, une caméra, des centaines de cartes d'identité avec photo vierge et l'arrière-fond utilisé pour prendre des photos pour les permis de conduire.[12]

Les médias ont rapporté qu'en septembre 2005, deux entrées par effraction ont eu lieu à quelques heures d'intervalle dans deux bureaux provinciaux du Ministry of Health Vital Statistics, l'une à Victoria et l'autre à Vancouver. Les autorités estiment que c'était une opération coordonnée. Au total, 1 000 certificats de naissance, de décès et de mariage vierges ont été volés. La police a déclaré que les criminels savaient dans quelle armoire les certificats étaient entreposés, ce qui pourrait indiquer des complices internes.[13]

Violations non ciblées

D'autres violations peuvent ou non être ciblées, mais elles n'en signifient pas moins des risques pour les données des clients.

La CIBC a publié un communiqué de presse selon lequel, à Montréal en janvier 2007, les Fonds mutuels Talvest, Gestion des actifs de la CIBC, ont annoncé qu'un fichier de sauvegarde renfermant « l'information relative au processus utilisé pour ouvrir et administrer environ 470 000 comptes clients courants et anciens de Talvest » avait disparu lors d'un transfert entre ses bureaux. Le fichier pourrait avoir inclus les noms, les adresses, les signatures, les dates de naissance, les numéros de compte bancaire, l'information sur les bénéficiaires et les NAS des clients. Le communiqué de presse déclarait que l'entreprise avertissait tous ses clients par lettre et se tiendrait responsable de toutes les pertes monétaires découlant de cette violation.[14]

Les entreprises ne peuvent fermer les yeux sur le fait que les renseignements personnels qu'elles possèdent intéressent les criminels. Les menaces proviennent de l'intérieur et de l'extérieur des entreprises. Compte tenu de cette menace, celles-ci doivent réévaluer leurs pratiques de sécurité à tous les niveaux (personnel, stockage des données, accès aux données, contrats accordés à des tierces parties avec accès aux données) pour atténuer les risques de perte des données des clients.

Corruption des employés

La corruption au sein des institutions publiques et privées affaiblit la confiance du public et de l'économie pour ces institutions. Pour les besoins du présent projet, il y a corruption lorsqu'un employé utilise son poste pour acquérir ou posséder de l'information sur les employés ou les clients ou en faire le trafic sans autorisation, ou utilise son poste pour commettre de la fraude.

Motivation

La plupart des employés des secteurs public et privé sont motivés par le gain financier.

Liens avec le CO

Les employés corrompus d'organismes gouvernementaux peuvent se bâtir une réputation de fournisseurs de services à des criminels.

Les employeurs doivent être sensibilisés à la valeur des renseignements personnels pour les criminels, aux facteurs de motivation qui permettent de corrompre les employés et aux indices qu'un employé peut être corrompu afin de réduire le risque que les données des clients et des employés soient compromises.

12 Adam Clayton, « Mounties fear theft done for id fraud: License gear stolen », The Winnipeg Sun, 2005-04-10, p. A5.
13 David Carrigg, « ID-theft ring suspected in twin break-ins », The Province, 16 septembre 2005.
14 Communiqué de presse corporatif de la CIBC, « Talvest Mutual Funds issues statement regarding missing back up computer file », Montréal, 18 janvier 2007.

Diligence raisonnable

Même si les institutions des secteurs public et privé sont ciblées par la fraude d'identité, un grand nombre sont vulnérables parce qu'elles ne font pas preuve de diligence raisonnable. Cela inclut des procédures d'embauche et de sécurité du personnel sécuritaires, l'entreposage et la transmission sécuritaires des données sensibles sur les clients et les employés et la protection et la vérification d'autres actifs. En règle générale, les aspects liés à la sécurité sont secondaires pour les industries motivées par le profit. Souvent, les entreprises hésitent à consacrer des ressources à des mesures de sécurité, à moins qu'elles ne risquent des pertes financières.

En 2006, une fraude hypothécaire a suscité l'indignation du public de l'Ontario, compte tenu du fait que la loi et les décisions des tribunaux de l'Ontario ont accordé plus de droits aux institutions prêteuses qu'aux propriétaires résidentiels dont le titre de propriété avait été fraudé et qui étaient donc considérés responsables des hypothèques, du fait de la fraude. Une décision d'octobre 2006 de la Cour supérieure de l'Ontario a tranché en faveur des propriétaires légitimes et dans certains cas, lorsque l'institution prêteuse ne fait pas preuve de diligence raisonnable, elle est responsable des pertes liées à la fraude hypothécaire.

Dans ce cas particulier, des fraudeurs se faisaient passer pour les propriétaires légitimes et un acheteur frauduleux, présentait des pièces d'identité falsifiées à un avocat qui, à son insu, facilitait le transfert du titre et la transaction avec l'institution prêteuse. Lorsque la fraude a été découverte, les propriétaires légitimes et la banque ont convenu que le couple devait être déclaré propriétaire légitime, mais ils ne se sont pas entendus sur la responsabilité du remboursement de l'hypothèque.

Le tribunal a statué que la banque n'avait pas fait preuve de diligence raisonnable. Elle avait échoué à détecter des signes de fraude en rapport avec le défaut de céder des espaces de stationnement et d'entreposage, le paiement de 30 000 $ au courtier hypothécaire pour une hypothèque type et l'absence de versement d'un dépôt. Avec des répercussions plus importantes, l'institution prêteuse n'avait pas mandaté un évaluateur de visiter la propriété, évaluateur qui, selon le juge « aurait découvert la fraude ».[15]

En décembre 2006, le gouvernement de l'Ontario a voté la Loi de 2006 sur la modernisation des services et de la protection du consommateur. La Loi 1) fait en sorte que les propriétaires légitimes ne perdront pas leur propriété à la suite de l'inscription d'une hypothèse falsifiée, d'une vente frauduleuse ou d'une procuration falsifiée, 2) rationalise la Caisse d'assurance des droits immobiliers, de manière à ce que dans les cas types de fraude, le titre soit restitué et une décision d'indemnisation prise dans les 90 jours et 3) augmente les amendes en cas de fraude sur les biens immobiliers de 1 000 $ à 50 000 $.[16]

Les lois sur la propriété relèvent de la compétence des provinces et donc, les lois qui régissent la fraude sur hypothèque et sur titres varient selon les provinces.

Législation sur la divulgation des violations de la sécurité

Dans la plupart des cas, les institutions ne possèdent pas les renseignements personnels des clients, elles n'en sont que les gardiennes. Fréquemment, les violations des données des clients ne sont pas signalées à ceux-ci ou aux organismes d'application de la loi, en raison du risque de répercussions négatives, comme la perte de clientèle, la dévaluation des actions ou les coûts associés à la divulgation de la vulnérabilité et à la prise de mesures de protection en conséquence. De plus, il n'existe aucune obligation de divulgation publique au Canada.

À l'heure actuelle, la notification des violations des renseignements personnels demeure une décision individuelle des entreprises au Canada. Aux États-Unis, nombre d'États ont voté une loi sur la divulgation des violations de la sécurité. Les individus qui sont informés que leurs renseignements personnels ont été violés peuvent prendre des mesures pour prévenir l'utilisation de cette information aux fins de fraude. La perte de contrôle ou l'impuissance ressentie par les victimes ont été bien documentées dans les cas de fraude d'identité; il s'agit d'une façon pour elles de récupérer un certain contrôle. De plus, les exigences de divulgation publique pourraient motiver les institutions à mieux protéger les renseignements personnels en leur possession.

Cette absence de législation a récemment été rendue publique à la suite des violations de l'information de cartes de crédit de Winners et HomeSense en janvier 2007 et de la disparition d'un fichier de sauvegarde renfermant les données de 470 000 clients de fonds d'investissement Talvest. Les enquêtes sur la violation de la sécurité menées par le Commissariat à la protection de la vie privée du Canada, comme celles concernant les Fonds d'investissement Talvest, ne sont pas juridiquement contraignantes et se limitent simplement à proposer des recommandations de changement.[17]

15 Ontario Superior Court of Justice; Rabi v. Rosu, 2006 CanLII 36623 (ON S.C.), 2006-10-31, 06-CV-311147

16 "Real estate fraud gives homeowners peace of mind," Queen's Park, February 5, 2007. www.gov.on.ca/MGS/en/News/112294.html

17 Michael Geist, « Identity theft in Canada », 2007-01-22. www.p2pnet.net/story/11084

Service à la clientèle ou sécurité

Dans la société techniquement avancée où les activités se déroulent à un rythme rapide, des pressions constantes sont exercées pour s'assurer que les services sont rendus de la manière la plus rapide, facile et économique possible. Au nombre des exemples figurent les tendances à adopter des applications en ligne pour les documents de sécurité canadiens, les prestations gouvernementales et les transactions bancaires en ligne.

Par contre, le renforcement des mesures de sécurité pour protéger les données, les renseignements personnels ou assurer l'intégrité des documents requièrent temps et ressources et peuvent s'avérer coûteuses. Souvent, les pratiques de sécurité sont évaluées et mises en œuvre en se fondant sur les principes de gestion des risques; les institutions évaluent les risques de perte ainsi que les coûts pour leurs opérations associés aux divers degrés de sécurité.

Le service à la clientèle et les exigences en matière de sécurité sont à l'évidence contradictoires. Le service à la clientèle vise à satisfaire les demandes des clients, comme l'octroi d'un crédit ou la délivrance de pièces d'identité, le plus rapidement et moyennant un tracas minime pour les clients, alors que la sécurité vise à éliminer le risque, ce qui généralement s'avère plus coûteux, fastidieux et long pour le client. La difficulté en bout de ligne consiste à trouver un équilibre.

Délits et condamnations

La fraude d'identité est considérée comme un délit sans victime, qui est peu sanctionné, parce que souvent, il y a absence de violence et du fait que les institutions financières remboursent aux victimes la plupart des pertes financières. Les faibles peines imposées ne sont pas un facteur de dissuasion, étant donné l'importance des profits réalisés. De ce fait, le taux de récidive chez les auteurs de délits de fraude d'identité est extrêmement élevé. Un certain nombre de suspects identifiés dans le cadre du présent rapport sont des criminels professionnels ou ils ont un casier judiciaire chargé.

Les délits de fraude d'identité font l'objet de poursuites en vertu des nombreuses dispositions concernant les délits du Code criminel du Canada (CCC). Une liste non exhaustive de 46 délits a été compilée pour la présente évaluation et figure en annexe A. Il n'existe aucun délit adéquat prévu par le CCC qui couvre l'acquisition, la possession ou le trafic non autorisés des renseignements personnels dans le but de commettre un acte criminel (les données des cartes de paiement et les passeports sont les exceptions).

Selon les données reçues dans le cadre du projet, les peines allaient de six ans avec une expulsion ultérieure à aucune condamnation. La peine de six ans était une sanction grave pour un cas de fraude d'identité au Canada.

La sanction la plus fréquente en cas de corruption des employés était le licenciement, qui a souvent lieu avant que la police ne soit invitée à enquêter. Dans au moins neuf cas, les employés ont fait l'objet d'accusations. Il n'y a pas eu suffisamment de données fournies au projet pour effectuer le suivi de ces accusations dans la plupart des cas.

Il n'y a pas suffisamment de données pour poursuivre l'évaluation des accusations et des condamnations, étant donné que nombre de fraudeurs déclarés coupables n'avaient pas reçu leur sentence au moment de la collecte, que certains cas étaient encore sous enquête, ou que les données n'étaient pas déclarées ou disponibles.

PhoneBusters, le Centre d'appel antifraude du Canada

PhoneBusters, le « Centre d'appels antifraude du Canada » est l'organisme central canadien qui réunit et collige les renseignements sur les plaintes relatives au marketing de masse, aux lettres de fraude sur les frais payables d'avance (lettres du Nigéria) et recense les plaintes pour vol. L'information est transmise aux organismes d'application de la loi pertinents, selon les priorités. Les données réunies par PhoneBusters constituent un outil précieux pour l'évaluation des répercussions de divers types de fraude sur le public. Elles aident également à prévenir de futurs délits similaires. Ce centre d'appels antifraude national est exploité par la Police provinciale de l'Ontario (OPP) en partenariat avec la GRC et le Bureau de la concurrence.[18]

Le « Signalement en direct des délits économiques » (centre RECOL) est une initiative en ligne qui permet aux particuliers de signaler des délits économiques et aux individus d'inscrire leurs plaintes en ligne. Ce service est administré par la GRC en partenariat avec l'OPP et Internet Fraud Complaint Center aux États-Unis.[19]

PhoneBusters et le centre RECOL procèdent à la fusion de leurs opérations sous l'égide du Centre d'appels antifraude du Canada.

PhoneBusters accède déjà à un réseau de contacts dans le secteur privé et au sein des organismes d'application de la loi canadiens et internationaux. Le centre fournit des pistes d'enquête aux organismes d'application de la loi de l'ensemble du pays, ainsi que des rapports statistiques et tactiques sur la fraude d'identité au Canada.

18 http://www.phonebusters.com/francais/aboutus.html
19 www.recol.ca

Sensibilisation et éducation du public

La sensibilisation et l'éducation du public sont essentielles du point de vue de la réduction du nombre des fraudes d'identité. Les secteurs de l'application de la loi, les secteurs public et privé et le secteur bénévole du Canada participent à de nombreuses initiatives de prévention des fraudes qui visent à sensibiliser la population de manière à minimiser les risques pour les particuliers d'être victimes de fraude. Toutefois, les victimes de fraude d'identité continuent à assumer la responsabilité du rétablissement de leurs réputations financière et personnelle.

L'éducation est un volet crucial des activités de PhoneBusters. Chaque individu qui communique avec le centre d'appels pour signaler une escroquerie ou une victimisation reçoit des renseignements, de manière à réduire ou minimiser le risque de compromission supplémentaire.

« La fraude. Identifiez-la. Signalez-la. Enrayez-la » est un slogan antifraude créé en 2005 par le Forum sur la prévention de la fraude (FPF). Le FPF, présidé par le Bureau de la concurrence, est un groupe intéressé d'entreprises du secteur privé, d'associations de consommateurs et de bénévoles et d'organismes gouvernementaux et d'application de la loi qui ont à cœur la lutte contre la fraude qui vise les consommateurs et les entreprises. Par l'éducation, il cherche à prévenir les fraudes dont sont victimes les Canadiens. Environ 90 entités participent à ce forum.[20]

Le FPF a désigné le mois de mars mois de prévention de la fraude au Canada. Les objectifs de cette campagne annuelle consistent à:

- livrer des messages qui sensibilisent le public à la fraude;
- aider les Canadiens à éviter de devenir des victimes et les encourager à signaler les fraudes;
- sensibiliser à la portée et à l'omniprésence des fraudes visant les consommateurs et les entreprises au Canada;
- faire du Canada un environnement hostile pour ces délits.

En même temps que le lancement du mois de la prévention de la fraude en 2007, la Sous-direction des délits commerciaux de la GRC a publié le guide Protection des renseignements personnels et protection contre l'escroquerie — Guide pratique canadien. Ce guide met l'accent sur la protection des renseignements personnels, décrit de nombreuses escroqueries, souligne les signaux d'alarme ou indices qui pourraient signifier une fraude et fournit aux lecteurs des outils et des liens pratiques pour réduire le risque qu'ils deviennent victimes de fraude. Cet outil de prévention des fraudes reprend le contenu du document qui l'a précédé, Guide pratique de l'étudiant, et il est disponible sur le site Web de la GRC à l'adresse http://www.rcmp-grc.gc.ca/scams/canadian_practical_guide_f.htm#mail.

Les stratégies d'éducation et de sensibilisation fournissent à la population les outils requis pour identifier et prévenir les stratagèmes de fraude qui évoluent constamment. Ces stratégies permettent aux individus de contrôler et de mieux protéger leurs renseignements personnels en remettant en question la nécessité de fournir ces renseignements à ceux qui les demandent (p. ex. les codes postaux aux détaillants), en apprenant à déchiqueter les documents et en précisant quels sont les renseignements personnels qu'on ne devrait pas conserver dans les portefeuilles, par exemple.

Toutefois, les campagnes de sensibilisation et d'éducation ne traitent pas ou ne suppriment pas la responsabilité qu'ont les institutions des secteurs public et privé de faire preuve de diligence raisonnable concernant les renseignements personnels et leurs compromissions.

20 www.fpf.ca

Conclusion

La présente évaluation démontre que les renseignements personnels sont devenus un produit de valeur pour les criminels. La triste réalité veut qu'à l'ère de l'électronique, nous ne sommes plus en mesure de recenser tous les emplacements où résident nos renseignements personnels. Les institutions des secteurs public et privé ainsi que les individus doivent donc manipuler et protéger l'information en tenant compte de ces faits.

Les entreprises ou institutions des secteurs public et privé doivent être sensibilisées à la valeur criminelle des renseignements personnels qu'elles possèdent et évaluer leurs pratiques de sécurité à tous les niveaux (personnel, stockage des données, accès aux données, sous-traitance avec accès aux données) de manière à atténuer les risques de perte des données sur les clients et les employés. Les menaces sont à la fois internes et externes.

Les enquêtes sur les délits de fraude d'identité requièrent la collaboration de multiples partenaires des organismes d'application de la loi, des pouvoirs publics et du secteur privé, en raison de la portée et de la nature de ces délits. Les enquêtes mentionnées dans le cadre du présent rapport bénéficiant de la coopération de multiples partenaires sont celles qui ont donné le plus de résultats.

Le Canada ne veut pas devenir un paradis pour les criminels internationaux qui se livrent à la fraude d'identité; pourtant, la faiblesse des sanctions pénales et l'importance des profits générés par les stratagèmes de fraude d'identité exposent le pays à des risques.

Ceci dit, les victimes assument actuellement la majorité des responsabilités en matière de rétablissement de leurs réputations financière et personnelle.

Nombre d'enquêteurs sur les fraudes et d'analystes de ces délits soutiennent que la fraude d'identité et les autres délits financiers constituent une faible priorité pour les secteurs d'application de la loi et de la justice pénale. Le crime organisé, le terrorisme, le trafic de stupéfiants et les délits avec violence se voient tous accorder la priorité. Pourtant, la fraude d'identité facilite tous ces délits.

Fait particulièrement inquiétant, le délit de fraude d'identité constitue une menace grave et immédiate pour l'intégrité de nos institutions publiques et privées : pour n'en nommer que quelques-unes, les banques, les institutions postales, les ministères gouvernementaux et les bureaux de crédit sont tous ciblés et compromis. Les victimes de fraude d'identité n'ont pas confiance en ces institutions. Ils critiquent notre incapacité en tant que société à protéger les individus contre les délits de fraude d'identité et à apporter des réponses adéquates. Tant que la portée globale et les répercussions individuelles de la fraude d'identité ne sont pas bien comprises, ce délit ne sera pas considéré comme grave.

Selon l'honorable juge S.C. Antifaev :

La possession de cartes de crédit, la possession de pièces d'identité, la modification de permis de conduire, pas seulement une fois dans le dernier cas, la possession de clés à boîtes aux lettres de Postes Canada constituent des délits extrêmement graves... Il s'agit, malheureusement, d'activités qui, si elles ne sont pas sanctionnées avec sévérité par le tribunal, vont entraîner des pertes totales de confiance du public en son système de courrier postal et en la validité du système d'octroi des permis de conduire, ainsi qu'un manque ou une perte de confiance du public et des intervenants du domaine financier en la validité des documents que nous considérons tous comme garantis, documents que nous utilisons tous dans la vie courante. Je fais référence non seulement aux pièces d'identité, mais à nos cartes bancaires, nos cartes de crédit et les documents de cette nature. Il s'agit de délits qui minent les fondements de notre vie au sein de la société. À moins que des mesures sérieuses ne soient prises pour contrer ces délits, à moins que les tribunaux et d'autres intervenants ne se penchent très sérieusement sur ces types de délits, qui, pour dire la vérité, constituent des délits de vol d'identité, il en découlera un affaiblissement de l'ensemble du tissu social sur lequel nous comptons tous.

R. c. Brian Christopher McNeil, 25-01-2006
Cour provinciale de la Colombie-Britannique

Annexe A — Infractions au CCC faisant généralement l'objet de poursuites en cas de fraude d'identité

Infraction	Disposition législative
Faux ou usage de faux en matière de passeport	Code criminel art. 57. (1)
Fausse déclaration relative à un passeport	Code criminel art. 57. (2)
Possession d'un passeport faux, etc.	Code criminel art. 57. (3)
Emploi frauduleux d'un certificat de citoyenneté	Code criminel art. 58. (1)
Abus de confiance par un fonctionnaire public	Code criminel art. 122
Omission de se conformer à une condition d'une promesse ou d'un engagement	Code criminel art. 145 (3)
Vol, etc. de cartes de crédit	Code criminel art. 342. (1)
Utilisation non autorisée de données relatives à une carte de crédit	Code criminel art. 342. (3)
Fabrication ou possession d'instruments destinés à fabriquer ou à falsifier des cartes de crédit	Code criminel art. 342.01 (1)
Utilisation non autorisée d'ordinateur	Code criminel art. 342.1 (1)
Possession de biens criminellement obtenus	Code criminel art. 354. (1)
Vol de courrier	Code criminel art. 356. (1)
Escroquerie : faux semblant ou fausse déclaration	Code criminel art. 362. (1)
Faux	Code criminel art. 366. (1)
Faux document	Code criminel art. 366. (2)
Emploi d'un document contrefait	Code criminel art. 368. (1)
Papier de bons du Trésor, sceaux publics, etc.	Code criminel art. 369
Proclamation contrefaite, etc.	Code criminel art. 370
Envoi de télégrammes, etc. sous un faux nom	Code criminel art. 371
Faux messages	Code criminel art. 372 (1)
Rédaction non autorisée d'un document.	Code criminel art. 374
Obtenir, etc. au moyen d'un instrument fondé sur un document contrefait	Code criminel art. 375
Contrefaçon de timbres, etc.	Code criminel art. 376. (1)
Contrefaçon d'une marque	Code criminel art. 376. (2)
Documents endommagés.	Code criminel art. 377. (1)
Infractions relatives aux registres	Code criminel art. 378
Fraude	Code criminel art. 380. (1)
Emploi de la poste pour frauder	Code criminel art. 381
Enregistrement frauduleux de titre	Code criminel art. 386
Vente frauduleuse d'un bien immeuble	Code criminel art. 387
Reçu destiné à tromper	Code criminel art. 388
Aliénation de biens avec l'intention de frauder des créanciers	Code criminel art. 392
Obtention frauduleuse de transport	Code criminel art. 393 (3)
Livres et documents	Code criminel art. 397. (1)
Falsifier un registre d'emploi	Code criminel art. 398
Faux relevé fourni par un fonctionnaire public	Code criminel art. 399
Supposition intentionnelle de personne	Code criminel art. 403
Représenter faussement un autre à un examen	Code criminel art. 404
Reconnaissance d'un instrument sous un faux nom	Code criminel art. 405
Contrefaçon d'une marque de commerce.	Code criminel art. 406
Substitution	Code criminel art. 408
Instruments pour contrefaire une marque de commerce	Code criminel art. 409. (1)
Autres infractions relatives aux marques de commerce	Code criminel art. 410
Emploi illégitime d'uniformes ou certificats militaires.	Code criminel art. 419
Méfait concernant des données	Code criminel art. 430. (1.1)

Annexe B — Glossaire

Cardeur :

Criminel qui se livre au « carding », c'est-à-dire à la fraude aux cartes bancaires, une forme de vol d'identité. Les cardeurs utilisent des listes de renseignements de carte de crédit et de débit pour commettre de multiples fraudes en effectuant des achats sans le consentement du détenteur original de la carte.

Fouille de poubelles :

Tamisage des rebuts commerciaux résidentiels pour trouver des articles utilisables; dans ce cas, de l'information.

Embosseur de cartes :

Ce matériel est utilisé pour ajouter de l'information digitale aux bandes magnétiques des cartes en plastique.

Adresse de protocole Internet (adresse IP) :

Numéro unique qu'utilisent les appareils pour l'identification et la communication mutuelles sur un réseau qui utilise la norme du protocole Internet.

Fraude par tirage à découvert :

La fraude par tirage à découvert consiste à retirer de l'argent d'un compte bancaire dans lequel il n'y a pas suffisamment de fonds pour couvrir le chèque.

Enregistreur de frappe :

Matériel ou applications logicielles qui enregistrent la frappe d'un utilisateur.

Programme ou logiciel malveillant :

Programme conçu délibérément pour saisir, modifier ou endommager des données ou changer le comportement d'un ordinateur sans la connaissance ou l'intention explicite de l'utilisateur. Les logiciels malveillants incluent les chevaux de Troie, les logiciels espions, les virus et les vers.

Renseignements personnels :

Pour les besoins du présent document, les renseignements personnels désignent tout élément ou combinaison de renseignements qui peut normalement être utilisée pour identifier de manière unique un individu dans le cadre de la livraison de produits et de services, de services gouvernementaux ou d'activités d'application de la loi. Autre possibilité, l'expression peut également désigner l'information désignée pour acquérir des renseignements supplémentaires sur un individu.

Hameçonnage :

Consiste à utiliser l'ingénierie sociale pour la messagerie électronique, de manière à provoquer une réaction impulsive immédiate des individus qui sont acheminés sur des sites Web frauduleux. En bout de ligne, l'objectif est d'acquérir des renseignements personnels ou confidentiels.

Ingénierie sociale :

Manipulation de la confiance d'une personne dans le but d'acquérir un avantage.

Polluriels :

Messages électroniques en nombre non sollicités ou non souhaités.

Mystification :

Modification de l'identification ou de l'information d'authentification afin de tromper le lecteur sur la véritable identité de l'auteur.

Données de personnes décédées :

Les renseignements personnels de personnes décédées qui sont utilisés par les faussaires pour se faire passer pour des personnes décédées ou usurper leur identité, de manière à commettre des fraudes.[21]

21 Définitions de la SDDC de la GRC, Protection des renseignements personnels et protection contre l'escroquerie - Guide pratique canadien, et wikipedia.org.

RCMP Criminal Intelligence

Identity Fraud in Canada