



ARCHIVED - Archiving Content

Archived Content

Information identified as archived is provided for reference, research or recordkeeping purposes. It is not subject to the Government of Canada Web Standards and has not been altered or updated since it was archived. Please contact us to request a format other than those available.

ARCHIVÉE - Contenu archivé

Contenu archivé

L'information dont il est indiqué qu'elle est archivée est fournie à des fins de référence, de recherche ou de tenue de documents. Elle n'est pas assujettie aux normes Web du gouvernement du Canada et elle n'a pas été modifiée ou mise à jour depuis son archivage. Pour obtenir cette information dans un autre format, veuillez communiquer avec nous.

This document is archival in nature and is intended for those who wish to consult archival documents made available from the collection of Public Safety Canada.

Some of these documents are available in only one official language. Translation, to be provided by Public Safety Canada, is available upon request.

Le présent document a une valeur archivistique et fait partie des documents d'archives rendus disponibles par Sécurité publique Canada à ceux qui souhaitent consulter ces documents issus de sa collection.

Certains de ces documents ne sont disponibles que dans une langue officielle. Sécurité publique Canada fournira une traduction sur demande.

**Évaluation de la menace :
Fraude en marketing de masse**



**La perspective canadienne —
novembre 2007**



Renseignements criminels

Le présent document appartient à la GRC. Il est prêté à votre service à titre confidentiel à condition qu'il ne soit pas reclassifié, copié, reproduit, utilisé ou autrement diffusé, en tout ou en partie, sans le consentement de l'expéditeur. Il ne doit pas être utilisé dans des affidavits, des procédures judiciaires ou des assignations à comparaître ou pour toute autre fin judiciaire ou juridique. La présente mise en garde fait partie intégrante du document et doit en accompagner tout extrait.



AVANT-PROPOS

Le présent rapport est le fruit d'une collaboration entre la Sous-direction des infractions commerciales et la Direction des renseignements criminels de la Gendarmerie royale du Canada (GRC).

La GRC tient à remercier tous les partenaires canadiens et internationaux qui ont contribué à cette évaluation de la menace associée à la fraude en marketing de masse.

Le Centre d'appel antifraude du Canada (CAAC), les membres des partenariats canadiens de répression de la fraude en marketing de masse et le Groupe de travail national sur la fraude par marketing de masse ont offert une collaboration inestimable.

Cette évaluation de la menace fut initiée afin d'appuyer la Stratégie nationale contre le marketing de masse frauduleux. Cette évaluation constituera la participation canadienne au Projet STOP PAYMENT, une évaluation internationale mixte de la menace liée à la fraude en marketing de masse.

Prière d'adresser toute question au sujet de cette évaluation à :

Gendarmerie royale du Canada
Sous-direction des infractions
commerciales
1200, promenade Vanier
Ottawa (Ontario)
K1A 0R2

ou

Gendarmerie royale du Canada
Direction des renseignements
criminel
1200, promenade Vanier
Ottawa (Ontario)
K1A 0R2



TABLE DES MATIÈRES

Résumé	1
Introduction	4
A. Historique – La réaction à la FMM	5
B. Activités criminelles de l’heure	7
Fraude par télémarketing, par Internet et par envois postaux massifs.	7
Vol d’identité lié à la FMM	7
Blanchiment d’argent.	8
Menaces, intimidation ou violence	8
C. Fréquence des activités criminelles	9
La prolifération de la FMM au Canada	9
Fraudes d’origine canadienne ciblant des Canadiens.	11
Profil des victimes	17
Principaux foyers de FMM au Canada.	20
Caractéristiques des activités exercées selon la région	22
Fraudes d’origine étrangère ciblant des Canadiens	24
Différences dans la fréquence d’activités criminelles déterminées	26
D. Types d’organisations et de groupes criminels	27
Locaux traditionnels de vente sous pression	27
Profil changeant des fraudeurs en marketing de masse.	27
Réseaux criminels ouest-africains	27
Difficultés inhérentes au repérage des groupes fraudeurs.	28
Sources de financement.	28
E. Principales techniques de fraude	29
Recours à des facilitateurs	29
Méthodes de sollicitation et pertes financières connexes	30
F. Réception et recyclage des produits de la FMM	32
Principaux moyens de recevoir les fonds envoyés par les victimes	32

TABLE DES MATIÈRES

Principaux moyens de recycler les fonds reçus des victimes	34
Services de paiement Internet.	35
Monnaies numériques.	35
Cartes de crédit prépayées.	35
Estimation du volume de recyclage des produits de la FMM	36
Identification de passeurs de fonds et de contrôleurs.	36
G. Pratiques exemplaires en vigueur pour réduire la fréquence de la FMM	37
Renseignement	37
Répression	38
<i>Partenariats et groupes de travail</i>	38
Perturbation	41
<i>Programme d'interception</i>	41
<i>Programme de visites sur place.</i>	41
Prévention et éducation.	41
Conclusion	42
Annexes	44
ANNEXE A — Les 12 principales arnaques signalées par des Canadiens en 2006	45
ANNEXE B — STRATAGÈMES CANADIENS CIBLANT D'AUTRES PAYS - 2006	47

RÉSUMÉ

La fraude en marketing de masse (FMM), méthode d'escroquerie en forte expansion depuis 10 à 15 ans, peut être le fait de criminels seuls ou organisés. Au Canada, la majorité des arnaques documentées concernent des loteries à frais anticipés, des chèques contrefaits envoyés dans le cadre de faux tirages au sort, des cartes de crédit, des prêts, des subventions gouvernementales, des répertoires d'affaires, des occasions de placement, des offres d'emploi et la vente de marchandises sur Internet.

Le Canada et les États-Unis reconnaissent la FMM comme un problème de criminalité transfrontalière depuis 1997. Parmi les interventions conjointes entreprises pour lutter contre la FMM, on note la création de six partenariats régionaux et la mise sur pied du Centre d'appel antifraude du Canada (CAAC), aussi appelé PhoneBusters. Tous ces partenariats exigent une coordination et une collaboration entre les organismes de réglementation et d'application de la loi aux échelons local, provincial, national et international.



Activités criminelles de l'heure

Les progrès au chapitre des technologies de communication, y compris Internet, les téléphones cellulaires, les services bancaires électroniques et les virements télégraphiques, ont fait de la FMM un problème de nature et de portée internationales. Bien que les activités de FMM commises par la poste et par téléphone demeurent une source de préoccupation, l'utilisation d'Internet comme moyen de perpétration devient de plus en plus courante. Grâce aux systèmes de voix sur IP (VoIP) et aux téléphones cellulaires prépayés, les fraudeurs en marketing de masse ont davantage de mobilité et peuvent exercer leurs activités à partir de n'importe où, avec l'indicatif régional et le numéro de téléphone de leur choix. Il est donc difficile pour la police de les identifier et de déterminer où ils se trouvent.

Des réseaux criminels international semblent s'être établis dans toutes les grandes villes canadiennes et pratiquent abondamment des activités de FMM internationales, se livrant à la distribution massive de faux instruments financiers par la poste et par messagerie sans égard aux frontières.

Le vol d'identité est un élément subtil de la FMM. Nombre d'invitations frauduleuses amènent les gens à divulguer des renseignements personnels, les exposant ainsi à l'usurpation de leur identité. Les renseignements personnels ainsi obtenus servent à faciliter des arnaques en cours et à dresser des listes de prospection, qui sont ensuite revendues à d'autres réseaux en vue d'autres activités frauduleuses.

La FMM est un commerce lucratif. Dans son rapport annuel de 2006-2007, le Centre d'analyse des opérations et déclarations financières du Canada (CANAFE) a signalé que les infractions de base liées à la fraude (fraude par carte de crédit ou de débit, fraude par télémarketing, etc.) étaient plus courantes que les affaires de drogue en 2006-2007.

Au Canada, certains crimes contre les personnes, tels que la formulation de menaces, l'intimidation et les agressions à l'endroit d'anciens employés, de victimes ou de témoins, ont été associés à la FMM. D'après les renseignements tirés d'enquêtes antérieures, certaines activités de FMM au Canada feraient l'objet de rackets de protection exploités.

Fréquence des activités criminelles

Pour les années 2004 à 2006, les statistiques du CAAC indiquent une hausse des pertes financières signalées relativement à des plaintes de FMM. De plus, le nombre d'appels reçus par le Centre a grimpé de près de 60 %, passant de 92 307 en 2005 à 146 393 en 2006.

À l'heure actuelle, la tendance qui prend le plus d'ampleur en matière de FMM est l'utilisation d'instruments financiers contrefaits ou modifiés (chèques et mandats). De mars à avril 2007, près de 30 % des plaintes déposées auprès du CAAC concernaient l'utilisation d'un faux instrument financier. Les arnaques documentées qui sont axées sur l'utilisation de faux chèques ont une portée internationale et de plus en plus sont exécutées au moyen de comptes bancaires en Asie pour faciliter le blanchiment d'argent.

Les activités de FMM basées au Canada ciblent principalement des résidents du Canada et des États-Unis et, dans une moindre mesure, du Royaume-Uni et d'autres pays anglophones. Dans les cas où des Canadiens ont signalé des activités de FMM pratiquées à l'extérieur du Canada, les fraudeurs se trouvaient surtout aux États-Unis, au Royaume-Uni et en Espagne.

L'Ontario, le Québec, la Colombie-Britannique et l'Alberta sont les principales régions où les réseaux de FMM sont actifs. Près de la moitié des adresses signalées se trouvent en Ontario. Des combines de loterie, de tirage, de subvention, de prêt et de carte de crédit sont exploitées dans toutes ces régions. Les arnaques aux répertoires et aux fournitures de bureau sont surtout basées à Montréal, et certaines à Toronto. En 2006, 73,9 % des plaintes reçues par le CAAC concernant des suspects canadiens venaient de consommateurs à l'étranger. Les escroqueries d'origine canadienne visent principalement des résidents des États-Unis.

Les plaintes reçues de Canadiens font état de sollicitations frauduleuses en provenance de 105 pays différents. Les moyens de communication tels que le courriel, les systèmes VoIP et le réseau Internet en général font qu'il est plus facile pour les criminels de prendre contact avec leurs cibles. La majorité des plaintes concernant des fraudes d'origine étrangère portent sur des sollicitations venues des États-Unis, du Royaume-Uni, de l'Espagne et du Nigéria.

Principales techniques de fraude

Des intermédiaires peuvent contribuer sciemment ou non à différents stades d'exécution des activités de FMM, par

exemple à l'organisation initiale de l'arnaque, au repérage d'éventuelles victimes, à la communication avec les personnes ciblées, à la réception des fonds transmis par les victimes et au blanchiment des produits de la fraude. Les intermédiaires varient selon la taille et le degré de complexité du groupe en cause.

De façon générale, au cours des trois dernières années, le télémarketing (appels directs) s'est classé au premier rang des méthodes de sollicitation pour ce qui est du nombre de cas signalés. Viennent ensuite les sollicitations par la poste, par Internet, dans la presse écrite et en personne.

Réception et blanchiment des produits de la FMM

Auparavant, les victimes transmettaient généralement leur argent aux fraudeurs par la poste, sous forme de chèque ou d'espèces. Aujourd'hui, les escrocs recourent de plus en plus à des compagnies de transfert de fonds pour recevoir l'argent de leurs victimes, surtout lorsqu'il s'agit de sommes de moins de 10 000 \$. Pour les montants de 10 000 \$ et plus, les chèques de banque et les virements télégraphiques interbancaires sont les méthodes de transfert les plus courantes. Lorsque Internet est le principal moyen employé pour communiquer avec les victimes et effectuer les transactions frauduleuses, les paiements se font habituellement au moyen de systèmes de paiement Internet.

Au plan du blanchiment d'argent, on note parmi les méthodes employées depuis un certain temps le schtroumpfage¹, le virement électronique, le recours aux entreprises de transfert de fonds ou de vente de titres négociables, les casinos, les cartes de crédit et le regroupement de fonds au moyen d'entreprises légitimes. Des enquêtes récentes ont aussi dégagé quelques tendances naissantes qui présentent un intérêt particulier pour le recyclage des produits de la FMM, dont l'utilisation de systèmes de paiement Internet, de cartes de crédit prépayées et de monnaie électronique.

Plusieurs enquêtes menées au Canada ont révélé que les activités de FMM peuvent produire des revenus considérables en relativement peu de temps. Par exemple, à Montréal, le Projet Coral² a mis au jour une entreprise criminelle qui avait généré plus de 30 M\$US en 18 mois. Le Projet EMPTOR, un groupe d'intervention dirigé par la GRC en Colombie-Britannique, a révélé un stratagème frauduleux géré par un couple de cette province qui vendait une protection pour carte de crédit à des clients américains, ce qui lui a permis de soutirer plus de 10 M\$ à des milliers de victimes.

1 Technique de blanchiment d'argent consistant à faire des dépôts inférieurs au seuil de déclaration dans divers comptes répartis parmi plusieurs banques.

2 Projet Coral – Voir le résumé de cas à la partie G, sous la rubrique « Répression ».

Pratiques exemplaires en vigueur pour réduire la fréquence de la FMM

PhoneBusters, maintenant connu sous le nom de Centre d'appel antifraude du Canada (CAAC), joue un rôle fondamental dans la sensibilisation aux stratagèmes de FMM et dans leur prévention. Il favorise aussi l'application de la loi axée sur le renseignement en recueillant de l'information sur les plaintes et sur les victimes de fraude, en l'analysant et en la communiquant aux services de police compétents. La centralisation de la réception des plaintes de fraude est essentielle à l'amélioration de l'échange d'information et de renseignements.

Au Canada, les six partenariats de lutte contre la FMM, qui comprennent trois groupes d'intervention mixtes à Montréal, Toronto et Vancouver, sont les principaux organes chargés d'enquêter sur les activités de FMM, de les perturber et de démanteler les réseaux qui en sont responsables. De nombreux dossiers transfrontaliers qui ont fait l'objet d'enquêtes conjointes des forces policières canadiennes et américaines ont été réglés avec succès devant les tribunaux depuis 1998.

Mars est le mois de la prévention de la fraude au Canada et partout dans le monde. Pendant cette période, les membres du Forum sur la prévention de la fraude (FPF) mettent l'accent sur la sensibilisation aux dangers de la fraude et sur l'éducation du public selon la devise « *Identifiez-la. Signalez-la. Enrayez-la.* »

Conclusion

La FMM demeure un problème au Canada et entraîne de graves préjudices pour les victimes, ici comme à l'étranger. Tandis que les activités de FMM se poursuivent au Canada, des arnaques semblables prennent de l'ampleur dans d'autres pays. La FMM est perçue dans le monde criminel comme une activité très lucrative à faible risque, donc une avenue intéressante pour les groupes du crime organisé.

Au Canada, les stratagèmes les plus courants sont, dans l'ordre : les combines de prix (loteries ou tirages), les possibilités d'emploi ou de travail à domicile, les offres d'argent provenant de l'étranger (fraudes 419), les offres de prêt et les arnaques aux paiements excédentaires (vente de marchandises). Ces dernières années, toutes ces formes de fraude ont été associées à l'utilisation d'instruments financiers contrefaits ou modifiés. Toutes ont une portée internationale.

INTRODUCTION



Au cours des 10 à 15 dernières années, la FMM a proliféré, non seulement du point de vue du nombre d'infractions ou de tentatives, mais aussi du point de vue du nombre et du type d'activités. Le problème semble maintenant avoir pris une dimension internationale et une ampleur mondiale. Cette forme de fraude peut être le fait de criminels seuls ou organisés. Plusieurs pays ont souligné les problèmes d'application de la loi que soulève la FMM et ont reconnu le besoin de privilégier une stratégie de répression coordonnée.

Forts des nouvelles méthodes de communication plus avancées, les criminels peuvent joindre un public beaucoup plus vaste, à une distance beaucoup plus grande.

La FMM a attiré l'attention des autorités policières au début des années 90 et est considérée comme un problème économique grave au Canada. Depuis 1997, elle est également reconnue comme un problème de criminalité transfrontalière entre le Canada et les États-Unis. De 1993 à 2006, plusieurs interventions mixtes ont été organisées pour combattre la FMM, dont la création de six partenariats régionaux et du CAAC, anciennement appelé Phonebusters. Toutes ces initiatives ont exigé une coordination et une collaboration entre des organismes de répression et de réglementation locaux, provinciaux, nationaux et internationaux.

Les activités de FMM pratiquées au Canada touchent les gens d'ici et d'ailleurs. Elles sont le fait de personnes qui agissent seules ou en groupes organisés. Il y a fort à parier que certains fraudeurs en marketing de masse frappent — et que certaines victimes sont bernées — à répétition.

Les activités de FMM observées au Canada ne ciblent pas uniquement des Canadiens et ne sont pas exercées uniquement par des Canadiens. Le présent rapport ne saurait ni exposer les modes de fonctionnement de tous les stratagèmes ni énumérer tous les groupes qui y participent.

Les fraudeurs en marketing de masse profitent des technologies de communication pour brouiller les pistes et accroître la portée de leurs activités à peu de frais. Les problèmes de compétence territoriale ont des effets sur le public, la police et les organismes gouvernementaux.

Selon certains enquêteurs, le principal élément dissuasif associé aux activités de FMM au Canada vient de la possibilité d'extradition aux États-Unis, où les peines d'emprisonnement peuvent être trois fois plus sévères qu'ici.

A. HISTORIQUE — LA RÉACTION À LA FMM

En 1993, la Police provinciale de l'Ontario (OPP) a lancé le Projet PhoneBusters après le signalement d'incidents de fraude par télémarketing ciblant des résidents de l'Ontario. Il en est ressorti que le télémarketing frauduleux ne touchait pas seulement l'Ontario, mais aussi le reste du Canada et les États-Unis. De 1993 à 1996, les activités policières dans le cadre du Projet PhoneBusters ont révélé que la fraude par télémarketing représentait un problème de criminalité croissant au Canada, ce qui a attiré l'attention d'organismes d'application de la loi tant nationaux qu'internationaux.

En 1997, une réunion entre l'ancien président Clinton et l'ancien premier ministre Chrétien sur la criminalité transfrontalière a marqué la création d'un groupe de travail binational sur la fraude transfrontalière par télémarketing. Ce groupe de travail, qui est plus tard devenu un sous-groupe du Forum sur la criminalité transfrontalière Canada-États-Unis, avait pour mandat d'examiner des façons de combattre l'expansion inquiétante de la fraude transfrontalière par télémarketing. Il a reconnu la fraude par télémarketing comme un problème grave et croissant et a relevé plusieurs tendances et activités connexes des deux côtés de la frontière³.

En 1998, deux groupes de travail ont été mis sur pied sous la direction de la GRC dans les principales villes canadiennes où s'exerçaient des activités télémarketing frauduleux, soit le Projet COLT à Montréal, et le Projet EMP TOR à Vancouver. Ce sont des projets mixtes qui misent sur la collaboration d'organismes de police et de réglementation du Canada et des États-Unis et dont le mandat consiste à enquêter sur les fraudeurs en marketing de masse basés au Canada puis à les traduire en justice.

En 1999, le FBI a lancé l'opération Canadian Eagle, qui visait à améliorer la coordination et la collaboration transfrontalières au sein des groupes d'intervention mixtes en y affectant des agents spéciaux chargés de travailler directement avec eux.

À cette époque, des modifications ont été apportées à la *Loi sur la concurrence* du Canada afin d'y incorporer un article sur le télémarketing frauduleux.

En 2000, des organismes d'application de la loi et de réglementation du Canada et des États-Unis ont formé l'Alliance stratégique de Toronto.

En 2001, la GRC est officiellement devenue un partenaire de PhoneBusters, alors connu sous le nom de Centre d'appel national PhoneBusters (CNAPB). En 2002, le CNAPB a ajouté à son effectif un groupe d'analyse doté de ressources de renseignement.

En 2003, le sous-groupe sur la FMM du Forum sur la criminalité transfrontalière a diffusé un rapport quinquennal faisant état des tendances de l'heure en matière de FMM. Ce rapport soulignait que la fraude transfrontalière avait augmenté considérablement de 1997 à 2002 et établissait un plan d'action pour surmonter les difficultés connexes, précisant qu'il s'agissait de la « fin du commencement »⁴.



3 <http://www.usdoj.gov/criminal/fraud/uscwgrtf.htm> (Report of the United States – Canada Working Group, United States – Canada Cooperation Against Cross-Border Telemarketing Fraud, novembre 1997.)

4 <http://www.securitepublique.gc.ca/prg/le/bs/massmfr-fra.aspx> (Groupe de travail binational sur les fraudes transfrontalières par marketing de masse, Rapport du procureur général des États-Unis et du solliciteur général du Canada, mai 2003)

Le sous-groupe a conclu que plusieurs formes de fraude transfrontalière par télémarketing avaient pris beaucoup d'ampleur de 1997 à 2002 : stratagèmes de promotion de prix et de loteries; propositions frauduleuses de prêts; offres frauduleuses de cartes de crédit à faible intérêt ou de plan de protection de carte de crédit. Il a par ailleurs souligné le rôle croissant du crime organisé dans les activités de télémarketing frauduleux d'origine canadienne. Parmi les autres constats présentés dans le rapport, mentionnons que les « plaintes pour fraude transfrontalière par Internet augmentent régulièrement depuis trois ans »; que « d'après les données des États-Unis et du Canada, le vol d'identité est devenu l'une des formes de crimes qui connaissent la croissance la plus rapide »; et que « les stratagèmes frauduleux ayant un lien avec l'Afrique [...] [sont] depuis longtemps un problème pour les services d'application de la loi au Canada, aux États-Unis et au Royaume-Uni ».

L'année 2004 a vu naître le Forum sur la prévention de la fraude (FPF), qui réunit des sociétés du secteur privé, des groupes de consommateurs et de bénévoles, des organismes gouvernementaux et des services d'application de la loi qui ont à cœur de lutter contre la fraude ciblant les consommateurs et les entreprises. Par l'intermédiaire de ses partenaires, le Forum, qui est présidé par le Bureau de la concurrence, cherche à empêcher les Canadiens de devenir des victimes de fraude en faisant de l'éducation axée sur sa devise : « *Identifiez-la. Signalez-la. Enrayez-la.*⁵ »

Entre 2003 et 2005, trois nouveaux partenariats ont été conclus au Canada pour maintenir et améliorer les initiatives de collaboration canado-américaines visant à combattre la FMM et pour tabler sur les succès obtenus à ce chapitre. À cette époque, des activités de FMM devenaient visibles à l'extérieur des secteurs où elles avaient déjà été observées.

Les trois partenariats en question sont le Partenariat de l'Alberta contre la fraude transfrontalière, l'Alliance stratégique de Vancouver et le Partenariat de l'Atlantique — Combattons la fraude transfrontalière.

De mars 2005 à mai 2006, la GRC et ses partenaires en application de la loi ont pris part à l'Opération Global Con. Cette initiative misait sur la collaboration et la coordination d'organismes policiers nationaux et internationaux afin de cibler des stratagèmes de marketing de masse ayant une portée internationale. Au Canada seulement, 372 accusations ont été déposées.

En 2005, le Groupe de travail national sur la fraude par marketing de masse (GTNFMM) a été formé à la suite de réunions officielles et non officielles tenues vers la fin de 2004 et en 2005. En mai 2006, le GTNFMM avait élaboré la stratégie nationale de lutte contre la FMM, qui visait le démantèlement, la perturbation et la neutralisation des réseaux de FMM basés au Canada. Pour atteindre cet objectif, le groupe de travail a défini trois objectifs stratégiques fondamentaux : accroître les risques et les coûts liés aux activités de FMM; renforcer l'efficacité des mesures de répression; atténuer la vulnérabilité des victimes. Le cadre stratégique se fonde sur quatre piliers : 1) une répression plus vigoureuse; 2) une sensibilisation accrue; 3) le resserrement des conséquences judiciaires; 4) l'amélioration des données nationales. Le GTNFMM tâchera d'atteindre ces objectifs en entreprenant plusieurs initiatives sur une période de trois ans, à l'aide des ressources disponibles.

5 http://www.bureaudelaconcurrence.gc.ca/epic/site/cb-bc.nsf/fr/h_00122f.html

B. ACTIVITÉS CRIMINELLES DE L'HEURE

Fraude par télémarketing, par Internet et par envois postaux massifs

Au cours de la dernière décennie, la réaction des organismes canadiens d'application de la loi à la FMM était fortement axée sur la reconnaissance de la fraude par télémarketing comme un problème de criminalité transfrontalière entre le Canada et les États-Unis. Les deux pays ont entrepris de nombreuses initiatives conjuguées pour lutter contre les activités de télémarketing frauduleux exercées à partir du Canada.

Si la plupart des gens accueillent avec plaisir les nouvelles technologies qui leur facilitent la vie, les organisations criminelles, elles, profitent de toute percée technologique et de toute nouvelle occasion d'affaires pour élargir leurs activités illégales. L'avènement d'Internet a certainement facilité l'exécution de stratagèmes frauduleux, puisqu'il permet aux arnaqueurs de joindre et de leurrer des centaines de millions de personnes. Bien que la FMM par la poste et par téléphone demeure une préoccupation, de plus en plus d'activités frauduleuses se commettent au moyen d'Internet.

L'utilisation de faux instruments financiers serait maintenant très courante dans les combines de FMM. Au cours des trois dernières années, soit de 2004 à 2006, le CAAC a documenté une hausse du nombre total d'incidents de FMM signalés dans l'ensemble du pays, sauf au Manitoba, aux Territoires du Nord-Ouest, au Nunavut et en Ontario. Cette hausse s'explique par l'utilisation de faux instruments financiers (chèques et mandats) et d'Internet dans un grand nombre d'arnaques, y compris dans le cadre de stratagèmes de frais anticipés (loteries, tirages, prêts, cartes de crédit, offres d'emploi, combines 419 d'Afrique occidentale) et de paiement excédentaire (vente de marchandises ou location de propriétés). Au cours de la dernière année, 30 % de toutes les plaintes signalées au CAAC concernaient l'utilisation de chèques ou de mandats contrefaits.

Vol d'identité lié à la FMM

Le vol et l'utilisation frauduleuse de renseignements personnels et financiers facilitent les activités de FMM.

Selon les plaintes documentées par le CAAC, les fraudeurs en marketing de masse font usage de stratagèmes trompeurs conçus spécialement pour obtenir des renseignements personnels et financiers auprès de victimes peu méfiantes. De nombreuses sollicitations frauduleuses incitent les victimes à divulguer des renseignements personnels à des criminels et à s'exposer ainsi au vol d'identité.

Une fois obtenues, les données personnelles servent à dresser des listes de prospection ou de « dupes » qui sont ensuite utilisées pour exécuter des arnaques. Ces listes sont aussi revendues à d'autres groupes criminels en vue de la perpétration d'autres types de fraude.

Le vol d'identité se commet au moyen de diverses combines subtiles conçues pour tromper ou frauder des particuliers naïfs partout dans le monde. Les escrocs usent de moyens de pression pour convaincre leurs victimes de fournir des renseignements personnels et bancaires sous un faux prétexte, par exemple en leur offrant l'admissibilité immédiate à un prix.



L'utilisation d'Internet et les progrès technologiques facilitent encore davantage ces stratagèmes. Les fraudeurs utilisent Internet pour convaincre un public peu averti de dévoiler des renseignements personnels. Certaines personnes soupçonnées de FMM utilisent aussi des logiciels espions permettant d'obtenir des renseignements personnels à l'insu des victimes.

Les fraudeurs en marketing de masse utilisent également des données obtenues frauduleusement pour réaliser des gains financiers, obtenir des biens ou des services et voyager sous le couvert de l'anonymat. Dans certains cas, ils créent des identités fictives ou usurpent des identités réelles afin de louer des véhicules ou d'acheter des billets d'avion pour des voyages intérieurs ou à l'étranger. À l'aide de ces données, les fraudeurs peuvent aussi présenter de fausses demandes de services de consommation (abonnement à un service de téléphonie cellulaire, branchement d'une ligne téléphonique, location de bureaux ou de cases postales, ouverture de comptes bancaires, etc.).

Il arrive également que les données ainsi obtenues servent à établir des identités fictives pour faciliter le virement télégraphique de fonds. Cela permet aux escrocs de transférer des fonds partout dans le monde de façon anonyme et d'en prendre livraison auprès de compagnies offrant des services de transfert de fonds.

Blanchiment d'argent

Dans son rapport annuel de 2006-2007⁶, le Centre d'analyse des opérations et déclarations financières du Canada, aussi appelé CANAFE, affirme avoir communiqué des renseignements à des organismes de police et de sécurité relativement à 193 cas suspects représentant une valeur globale de près de 10 G\$. Les conclusions qui y sont formulées en ce qui concerne les tendances et les modes opératoires sont particulièrement intéressantes : « Les infractions de prédictat liées à la fraude (p. ex. fraude de carte de crédit et de débit, **fraude de télémarketing**) ont été plus fréquentes en 2006-2007 comparativement aux années précédentes, alors que la plupart des cas présumés de blanchiment d'argent était reliée [*sic*] à des infractions de trafic de stupéfiant. »

Dans un communiqué de presse daté du 25 octobre 2007, Horst Intscher, directeur de CANAFE, a affirmé que, cette année, pour la première fois, les affaires de **fraude** étaient probablement plus nombreuses que les affaires de **drogue**. À son avis, bon nombre de ces cas de **fraude** sont aussi pernicieux que n'importe quelle affaire de

drogue, puisqu'ils ciblent des personnes âgées au moyen de stratagèmes de **télémarketing** et de paiement anticipé pour des services qui ne sont jamais rendus. Par le passé, une forte proportion des dossiers de CANAFE concernait les produits du narcotrafic, **mais la fraude est maintenant le principal élément commun des transactions douteuses.**

Menaces, intimidation ou violence

Au Canada, la FMM a été associée à certains crimes contre la personne, tels que la formulation de menaces, l'intimidation et les agressions à l'endroit d'anciens employés, de victimes ou de témoins. Les anciens employés d'entreprises de vente sous pression sont nombreux à affirmer que leurs patrons usaient de menaces et d'intimidation pour les convaincre de ne pas dénoncer les activités illégales du groupe. On constate aussi des indications de la participation de gangs de rue à des activités de FMM.

Il arrive que des réseaux de fraude ouest-africains persuadent leurs victimes canadiennes de se rendre dans des pays étrangers, où elles risquent de subir d'autres pertes financières ou même des blessures. Par exemple, en 2007, un Canadien victime d'une fraude amoureuse s'est rendu au Ghana dans l'espoir de rencontrer une femme dont il avait fait la connaissance sur Internet. Il y a loué une chambre d'hôtel pendant plusieurs semaines. Au cours de cette période, on lui a escroqué plusieurs milliers de dollars. Un de ses voisins au Canada, auprès duquel il avait essayé d'emprunter de l'argent, a soupçonné qu'il était victime de fraude et a signalé l'affaire au CAAC. L'agent de liaison de la GRC a réussi à déterminer où l'homme se trouvait au Ghana, et le service de police local lui a porté secours. D'après les renseignements reçus au sujet de cette affaire, des suspects se seraient présentés à l'hôtel à la recherche de la victime à peine quelques minutes après son départ.

Certaines activités de FMM au Canada sont ciblées par des rackets de protection. Les arnaqueurs seraient tenus de verser un pourcentage de leurs profits à ces groupes pour exercer leurs activités dans certains secteurs.

6 <http://www.fintrac.gc.ca/publications/ar/2007/1-fra.asp>

C. FRÉQUENCE DES ACTIVITÉS CRIMINELLES

La prolifération de la FMM au Canada

De par sa nature même, le marketing de masse vise à atteindre le plus vaste public possible afin d'optimiser les profits. Or, la mondialisation et d'autres facteurs comme l'avènement d'Internet et l'introduction des systèmes VoIP ont effacé les frontières. La FMM est donc fondamentalement un problème de criminalité mondiale. C'est pourquoi des instances telles que l'Organisation de coopération et de développement économiques (OCDE) et le Réseau international de contrôle et de protection des consommateurs (RICPC) s'emploient maintenant à établir des lignes directrices et des groupes de travail qui ciblent tout particulièrement les stratagèmes de FMM⁷.

La FMM et les infractions commerciales connexes représentent une menace très grave pour notre économie. Les crimes de ce genre peuvent causer d'énormes pertes financières à leurs victimes, parmi lesquelles figurent des gouvernements, des institutions financières, des entreprises et des particuliers. Cela ébranle la confiance du public et des investisseurs dans les institutions et les processus établis et entraîne une augmentation des coûts pour le consommateur.

À l'heure actuelle, les plaintes relatives à la FMM sont recueillies par les organismes d'application de la loi du pays entier, par les partenariats de lutte contre la FMM, par le Bureau de la concurrence et par des organismes de réglementation provinciaux. Il est donc difficile de déterminer l'ampleur ou l'impact de la FMM au Canada.

Devant cette réalité, et comme tous les intervenants concernés connaissent les données du CAAC, les utilisent de façon généralisée et y attribuent une grande crédibilité, la majorité des données qui ont servi à la présente évaluation ont été obtenues auprès du CAAC. Ces données ne devraient toutefois être considérées que comme un instantané de la situation générale de la FMM au Canada.

Pour les besoins du présent rapport, on a obtenu des données sur les plaintes de consommateurs d'une variété des sources publiques et policières. Ainsi, comme nous l'avons mentionné plus haut, le présent rapport se fonde principalement sur les données fournies par le CAAC pour brosser un tableau de la FMM au Canada.

Comme la saisie de données sur les plaintes de FMM ne se fait pas de la même manière dans tous les systèmes, il n'est pas possible de décrire chacun des différents stratagèmes utilisés. De plus, ces stratagèmes sont flexibles; les fraudeurs peuvent mettre au point une sollicitation pour n'importe quel produit, service ou événement, comme en témoignent les combines qui ont vu le jour à la suite d'événements tragiques tels que la fusillade qui a tué quatre membres de la GRC à Mayerthorpe, les attentats du 11 septembre et l'ouragan Katrina. À peine quelques jours après ces événements, de nouveaux stratagèmes ont été lancés afin de solliciter des fonds pour de fausses œuvres caritatives⁸.



7 <http://www.icpen.org/ricc/apropos.htm>

http://www.oecd.org/document/53/0,3343,fr_2649_34267_2516463_1_1_1_1,00.html

8 http://news.com.com/Online+scams+emerge+in+Katrinas+wake/2100-7349_3-5845695.html

<http://www.cbsnews.com/stories/2005/09/09/katrina/main829212.shtml>

http://www.rcmp-grc.gc.ca/ab/news/2005/Mayerthorpe_VictimFund_Apr11-05_NR17.htm

Les escroqueries par marketing de masse sont des infractions financières et visent la réalisation de profits. Bien entendu, les stratagèmes employés varient du point de vue du degré de complexité, des organismes en cause et des sommes d'argent sollicitées. Il reste toutefois que ce sont des fraudes graves qui ont des répercussions sur le Canada.

L'analyse de la FMM dans une perspective canadienne peut se faire en fonction de deux grands thèmes : les activités de FMM d'origine canadienne qui ciblent des victimes canadiennes et étrangères, et les Canadiens victimes d'activités de FMM exercées à l'étranger. Les activités de FMM basées au Canada ciblent surtout des résidents du Canada et des États-Unis, et dans une moindre mesure, du Royaume-Uni et d'autres pays anglophones. D'après les plaintes déposées par des Canadiens, les activités de FMM qui ciblent des Canadiens à partir de pays étrangers sont basées surtout aux États-Unis, au Royaume-Uni et en Espagne.

De 2004 à 2006, les statistiques compilées par le CAAC indiquent que les pertes financières globales signalées dans les plaintes de Canadiens victimes de FMM étaient passées de 19 174 234,48 \$ à 25 916 962,36 \$. Le nombre d'appels reçus par le Centre a également grimpé de près de 60 %, passant de 92 307 en 2005 à 146 393 en 2006.

	Appels reçus	Appels traités
2005	92 307	76 770
2006	146 393	104 002

Les données fournies par le Consumer Sentinel et le Centre de SDDE dénotent une tendance semblable : de 2004 à 2006, le nombre de cas de FMM signalés a augmenté considérablement. Le Centre de SDDE affirme avoir reçu 3 439 plaintes en ligne en 2004, comparativement à 5 500 en 2006. Pour sa part, le Consumer Sentinel a reçu 64 892 plaintes de fraude transfrontalière en 2004, contre 95 249 en 2006.

Les activités de FMM

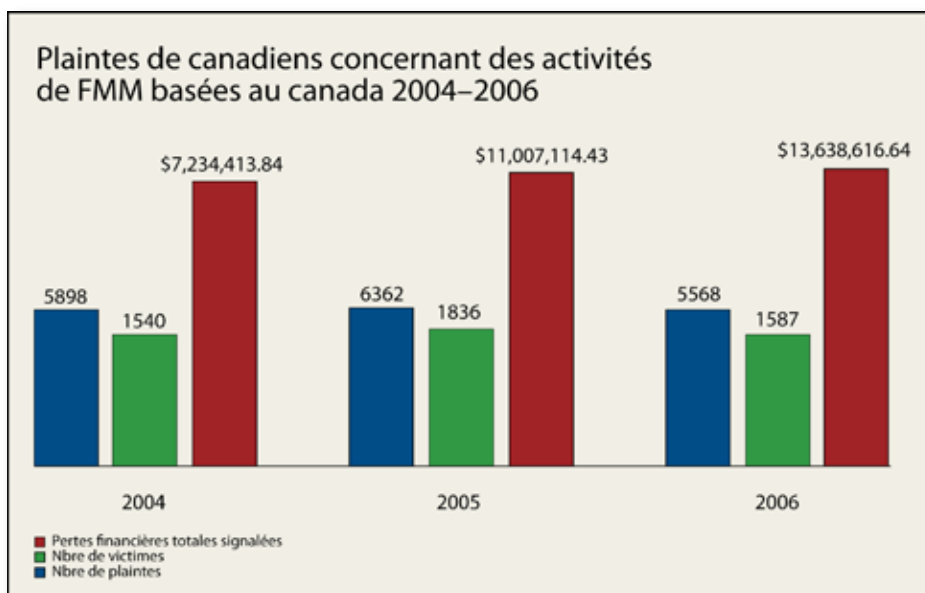


Fraudes d'origine canadienne ciblant des Canadiens

Les lieux où s'exercent les activités de FMM sont déterminés à partir des adresses suspectes fournies par les consommateurs. Il convient donc de noter que, dans certains cas, les adresses mentionnées peuvent être de simples adresses postales qui ne correspondent pas à l'emplacement physique d'un groupe de FMM, ou bien les coordonnées fournies pour le suspect peuvent être fictives. Il arrive aussi que le consommateur ne connaisse pas l'adresse du suspect ou que celle-ci ne lui ait jamais été communiquée.

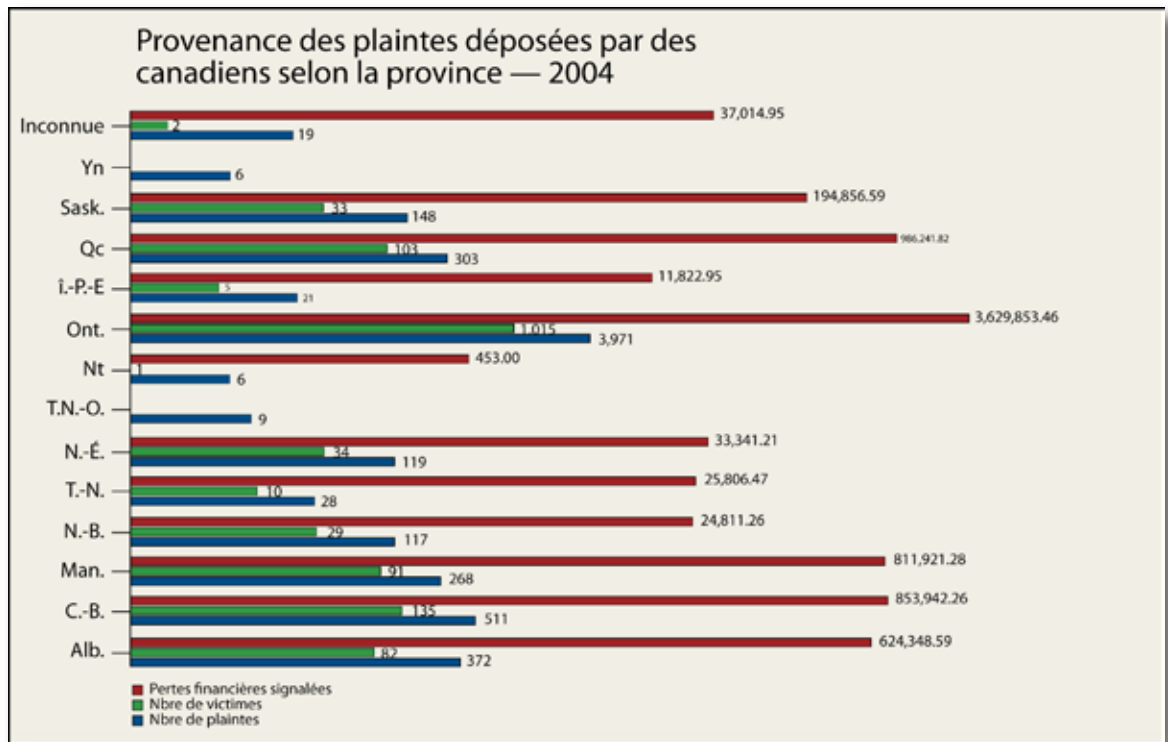
Les Canadiens qui affirment avoir fait l'objet d'une sollicitation par des fraudeurs en marketing de masse basés au Canada représentent en moyenne 37,89 % du nombre de plaintes reçues annuellement de 2004 à 2006. Le nombre global de plaintes est resté relativement stable. Toutefois, les pertes financières signalées pendant la même période ont presque doublé (graphique 1).

Graphique 1

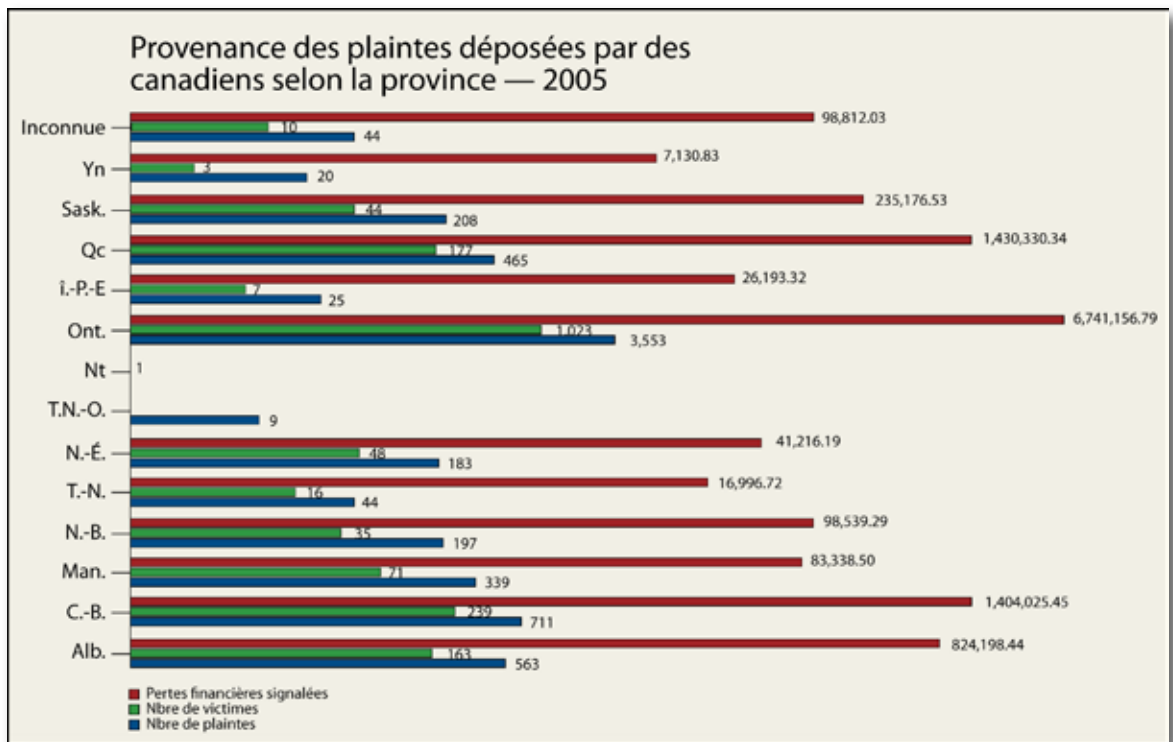


Voici la ventilation de ces chiffres par province (graphiques 2-4)

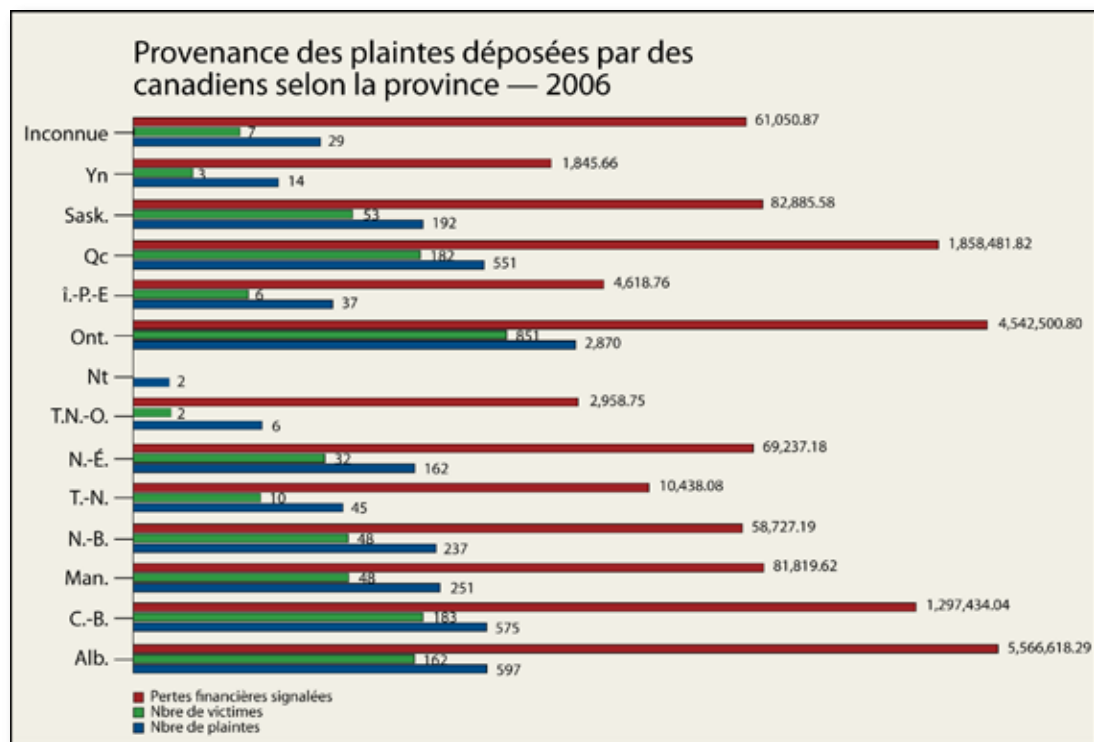
Graphique 2



Graphique 3



Graphique 4



Les chiffres présentés ci-dessus ont été signalés au CAAC par les provinces de 2004 à 2006. Pendant cette période, les cinq provinces les plus ciblées par les activités de FMM basées au Canada étaient l'Ontario, la Colombie-Britannique, le Québec, l'Alberta et le Manitoba. Dans l'ensemble, le nombre de cas signalés a augmenté partout sauf au Manitoba, dans les Territoires du Nord-Ouest, au Nunavut et en Ontario. Le CAAC reçoit généralement plus d'appels des provinces les plus peuplées.

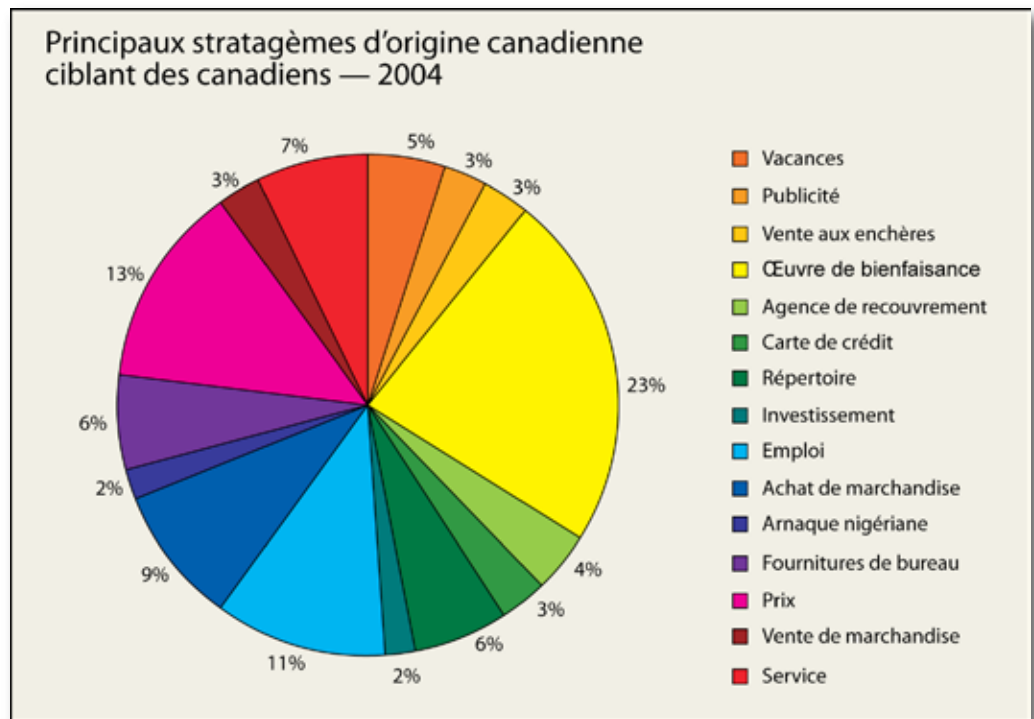
Au cours des trois dernières années, les signalements de la part de consommateurs en Ontario ont représenté en moyenne 58,24 % des plaintes reçues au CAAC. Ce pourcentage est attribuable en partie au fait qu'environ le tiers de la population du Canada habite en Ontario et que le CAAC est situé dans cette province. Bon nombre des initiatives de sensibilisation menées par le CAAC et SeniorBusters dans le passé se concentraient sur l'Ontario, puisque le programme était géré par l'OPP. Il importe aussi de souligner que de 2004 à 2006, le pourcentage de plaintes en provenance de l'Ontario a chuté de 67,33 % à 51,54 %, en raison des efforts de sensibilisation déployés à l'extérieur de l'Ontario sous la coordination du Forum pour la prévention de la fraude. De plus, l'étude commandée par le Bureau de la concurrence en 2004 a révélé que PhoneBusters n'était pas bien connu partout au Canada.

Les graphiques présentés ci-dessous illustrent, pour les années 2004 à 2006, les 15 stratagèmes les plus courants employés au Canada pour cibler des Canadiens. Parmi les principales tendances relevées à cet égard par le Groupe d'analyse des renseignements du CAAC pendant cette période, on note les offres de prêts frauduleux et les arnaques associées à la fraude traditionnelle de souche ouest-africaine (fraudes 419), qui sont en hausse. Par le passé, les combines de prêt ciblaient généralement les consommateurs américains au moyen d'annonces dans les journaux, mais la sollicitation se fait maintenant plutôt au moyen d'annonces en ligne et de sites Web.

Bien que les sollicitations relatives à de fausses œuvres caritatives se soient systématiquement classées au premier ou au deuxième rang des FMM ces trois dernières années, le nombre d'incidents signalés a diminué considérablement en 2006. Les analystes du CAAC soulignent que bon nombre des appels concernant des œuvres caritatives viennent de consommateurs qui s'enquêtent de leur légitimité, ce qui n'en fait pas nécessairement des stratagèmes de FMM.

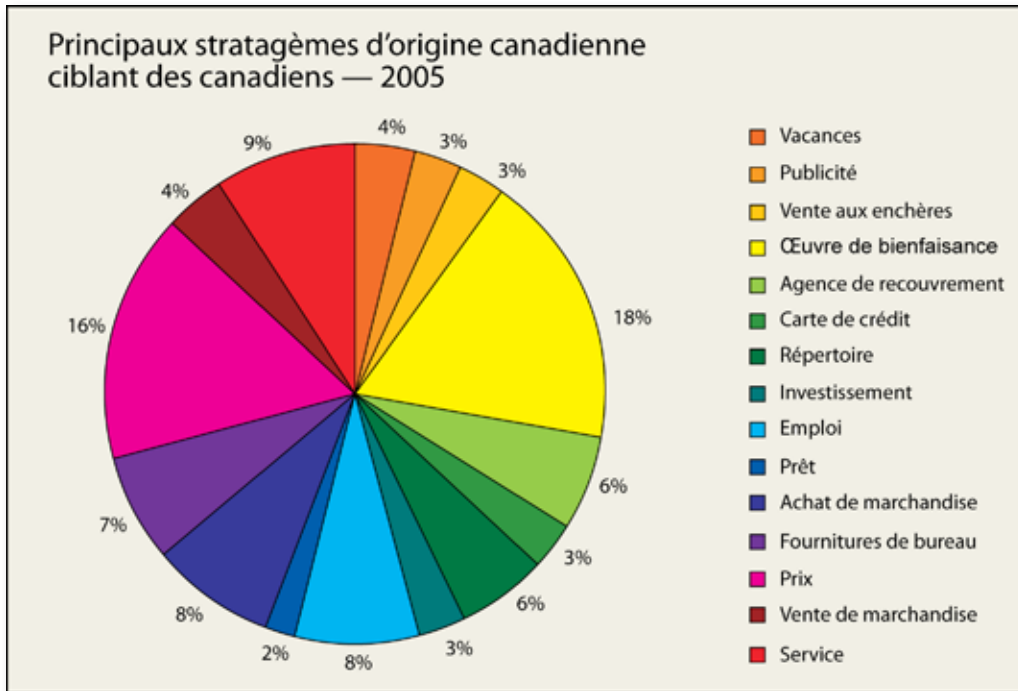
On constate une hausse du nombre de signalements ayant trait à des arnaques de prix, de répertoire, de service, de fournitures de bureau, d'agence de recouvrement, de paiement excédentaire, de placement et de prêt. Selon les membres du Groupe d'analyse des renseignements du CAAC, l'augmentation des sollicitations relatives aux prix et aux paiements excédentaires est liée à l'utilisation d'instruments financiers contrefaits ou modifiés⁹. La multiplication des offres de prêt est associée à l'utilisation d'Internet comme moyen de publicité.

Graphique 5

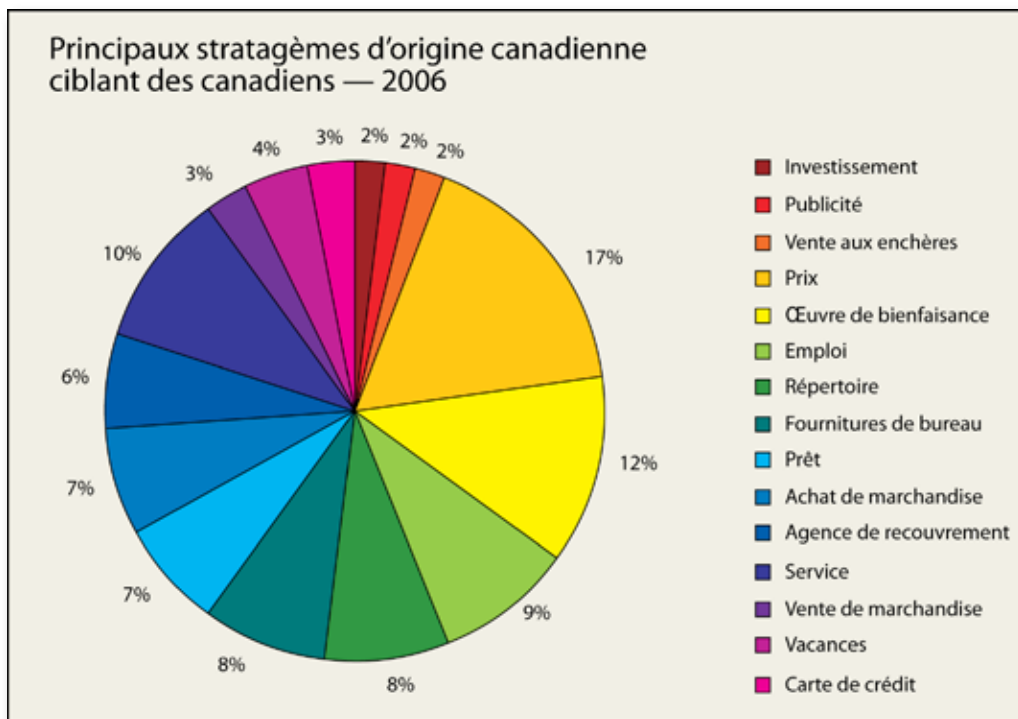


⁹ Il n'existe présentement aucune base de données au Canada qui puisse fournir de l'information sur les stratagèmes impliquant l'utilisation d'instruments financiers contrefaits ou modifiés.

Graphique 6



Graphique 7



Le tableau suivant fait état des principaux types de stratagèmes signalés au CAAC en 2006, ventilés selon la province de résidence du plaignant.

Tableau 2

	Alb.	C.-B.	Man.	N.-B.	T.-N.	N.-É.	T.N.-O.	Nt	Ont.	Î.-P.-É.	Qc	Sask.	Yn	Total
Prix	83	85	29	34	7	32			342	5	31	40	1	689
Oeuvre de bienfaisance	85	57	22	12	1	15			258	4	10	34	1	499
Emploi	25	34	8	13	1	8			252	2	23	7		373
Répertoire	26	17	16	4	3	4		2	135	1	99	14	3	324
Fournitures de bureau	33	32	12	9	2	2			116	4	96	9		315
Prêt	51	49	16	21	3	14	3		113	6	16	14		306
Achat de marchandise	34	25	12	7	5	5			142		36	5		271
Agence de Recouvrement	21	33	11	17	5	12			105		15	5	2	226
Service	27	32	13	6	1	9	1		298		32	7	1	427
Vente de marchandise	2	20	6	2	1	4			66		11	2		134
Vacances	27	12	20	21	1	12			69	2	1	7		172
Carte de crédit	10	16	11	3		5			46		15	6	1	113
Investissement	17	11	3	1	1	2			45	1	15	3		99
Publicité	7	5	1	2	1		1		40	5	13	2		77
Vente aux enchères	5	7	2	1		1			38	1	7	2		64

Profil des victimes

Les fraudeurs en marketing de masse ne font généralement pas de discrimination parmi leurs victimes. Certains groupes démographiques peuvent cependant être plus vulnérables à des types de stratagèmes et à des modes de sollicitation particuliers. Le Centre de SDDE et le CAAC ont tous deux reçu des plaintes d'hommes et de femmes dont l'âge se situait entre 18 et 100 ans. Un rapport diffusé par l'Office of Fair Trading du Royaume-Uni dément le mythe voulant que seules les personnes vulnérables, âgées ou naïves se font prendre par les arnaqueurs et confirme que moins de 5 % des gens signalent les escroqueries aux autorités. Toujours selon ce rapport, si les hommes et les femmes ont des chances égales d'être ciblés par un escroc, les incidents varient selon le type de combine¹⁰.

Pour ce qui est du nombre de victimes, les méthodes de sollicitation en personne¹¹, par la poste, par Internet et dans la presse écrite sont les plus efficaces pour les fraudeurs en marketing de masse établis au Canada qui cherchent à bernier des Canadiens. Selon les données analysées à ce jour, les stratagèmes de télémarketing resteront probablement la principale méthode de sollicitation signalée au CAAC, et il est très probable que les arnaques par la poste et par Internet continueront de prendre de l'ampleur en 2008.

Les données présentées dans les trois tableaux suivants montrent que les fraudeurs qui misent sur les appels téléphoniques directs¹² obtiennent des résultats particulièrement fructueux lorsqu'ils s'adressent à des septuagénaires ou à des octogénaires, et que ceux qui utilisent les services postaux obtiennent les meilleurs résultats avec les octogénaires et les nonagénaires, d'après les pertes financières signalées pour ces deux groupes d'âge.

10 Étude de l'Office of Fair Trading concernant les répercussions des arnaques sur les consommateurs du Royaume-Uni, décembre 2006, p. 10-11

11 En juin 2006, le CAAC a reçu une plainte concernant une perte de cinq millions de dollars à la suite d'une combine vieille de 10 ans, qui consistait à solliciter des investissements en personne.

12 Les « appels directs » constituent du télémarketing.

Tableau 3

Groupe d'âge	APPELS DIRECTS			POSTE			PRESSE ÉCRITE		
	Tentatives	Victimes	Pertes Financières Signalées	Tentatives	Victimes	Pertes Financières Signalées	Tentatives	Victimes	Pertes Financières Signalées
10 – 19	14	3	4 310,00 \$	2	3	167,80 \$	2	3	2 594,00 \$
20 – 29	139	24	48 393,48 \$	28	13	7 119,95 \$	10	30	20 863,58 \$
30 – 39	203	25	67 293,99 \$	34	13	4 793,89 \$	14	37	47 004,02 \$
40 – 49	276	34	155 808,49 \$	76	19	8 225,29 \$	25	48	27 425,90 \$
50 – 59	270	32	127 927,90 \$	67	24	1 548,10 \$	21	26	18 426,88 \$
60 – 69	269	36	110 728,95 \$	69	36	5 831,52 \$	11	15	16 913,93 \$
70 – 79	234	44	239 040,66 \$	85	28	7 765,61 \$	2	7	56 535,95 \$
80 – 89	86	33	214 068,00 \$	54	29	282 252,33 \$	0	4	159,85 \$
90 - 99	6	3	6 550,00 \$	13	4	302 862,45 \$	0	0	0 \$
ENTREPRISE	631	151	257 500,54 \$	85	12	4 796,09 \$	2	4	65 795,65 \$
INCONNU	449	66	29 265,55 \$	118	44	29 465,65 \$	28	16	255 934,95 \$
TOTAUX :	2 577	451	1 260 887,56 \$	631	225	654 828,68 \$	115	190	511 654,71 \$

Tableau 4

Groupe d'âge	INTERNET / COURRIEL			TÉLÉCOPIEUR			EN PERSONNE		
	Tentatives	Victimes	Pertes Financières Signalées	Tentatives	Victimes	Pertes Financières Signalées	Tentatives	Victimes	Pertes Financières Signalées
10 – 19	8	11	4 461,00 \$	0	0	0 \$	0	2	1 491,95 \$
20 – 29	62	102	97 628,71 \$	0	0	0 \$	6	20	681 911,88 \$
30 – 39	65	98	264 734,39 \$	1	0	0 \$	9	34	443 295,36 \$
40 – 49	60	76	101 869,08 \$	1	0	0 \$	17	29	1 352 865,43 \$
50 – 59	40	48	138 751,44 \$	1	1	295 000,00 \$	8	24	761 670,47 \$
60 – 69	23	22	68 437,41 \$	1	0	0 \$	6	14	5 167 710,00 \$
70 – 79	5	7	11 037,90 \$	1	0	0 \$	3	17	183 518,00 \$
80 – 89	2	1	4 500,00 \$	0	0	0 \$	2	13	270 386,25 \$
90 – 99	0	0	0 \$	0	0	0 \$	0	1	0 \$
ENTREPRISE	32	19	88 791,12 \$	18	2	0 \$	11	20	126 509,28 \$
INCONNU	46	32	38 264,30 \$	0	0	0 \$	27	20	419 165,50 \$
TOTAUX :	343	416	818 475,35 \$	23	3	295 000,00 \$	89	194	9 408 524,12 \$

Tableau 5

Groupe d'âge	AUTRE / INCONNU			RENVOI			TÉLÉVISION / RADIO / MÉDIAS		
	Tentatives	Victimes	Pertes Financières Signalées	Tentatives	Victimes	Pertes Financières Signalées	Tentatives	Victimes	Pertes Financières Signalées
10 – 19	0	1	939,84 \$	0	2	1 367,00 \$	0	1	350,00 \$
20 – 29	8	3	5 295,00 \$	1	0	0 \$	1	0	0 \$
30 – 39	6	7	35 121,89 \$	1	4	61 450,02 \$	0	1	259,00 \$
40 – 49	9	8	148 531,77 \$	4	3	36 465,00 \$	2	0	0 \$
50 – 59	9	7	1 126,59 \$	1	1	1 000,00 \$	1	2	401,80 \$
60 – 69	10	8	184 906,86 \$	2	1	851,00 \$	2	0	0 \$
70 – 79	2	5	11 300,00 \$	0	1	2 000,00 \$	3	3	785,20 \$
80 – 89	2	3	157,75 \$	0	0	0 \$	0	1	34,97 \$
90 – 99	0	0	0 \$	0	0	0 \$	0	0	0 \$
ENTREPRISE	31	12	57 229,09 \$	0	0	0 \$	0	0	0 \$
INCONNU	63	19	112 796,17 \$	1	1	5 000,00 \$	2	1	300,00 \$
TOTAUX :	140	73	557 404,96 \$	10	13	108 133,02 \$	11	9	2 130,97 \$

Les consommateurs les plus touchés par les stratagèmes de télémarketing sont âgés de 30 à 79 ans. Le nombre de victimes et de plaintes est le plus élevé chez les 30 à 49 ans. Fait intéressant, le taux de plaintes chez les moins de 50 ans est assez près de celui qu'on enregistre chez les personnes de plus de 50 ans. Quarante-huit pour cent des plaintes reçues venaient de consommateurs âgés de moins de 50 ans, et 52 %, de personnes âgées de plus de 50 ans.

Si l'on compare la situation des particuliers à celle des entreprises, on voit que 22 % du nombre total de plaintes reçues par le CAAC relativement au télémarketing venaient d'entreprises, tandis que 15 % venaient de plaignants qui n'avaient pas précisé leur groupe d'âge.

Les stratagèmes de sollicitation par la poste ont principalement touché les personnes âgées de 60 à 80 ans, et la majorité des victimes ainsi bernées étaient sexagénaires. À en juger par l'augmentation des sollicitations par la poste de 2004 à 2006, les combines de ce type continueront probablement de cibler les aînés dans les années à venir.

Les stratagèmes de fraude par Internet ont surtout touché les consommateurs de 20 à 60 ans, et la majorité des victimes ainsi bernées étaient dans la vingtaine. Il faudra pousser plus loin l'analyse des données pour déterminer quelles combines sont associées à Internet.

Les arnaques sur Internet permettent aux fraudeurs d'exercer leurs activités à partir de n'importe où. Les stratagèmes documentés sont exploités autant par des individus que par des organisations criminelles. Par exemple, les ventes aux enchères frauduleuses sur Internet peuvent être le fait d'une personne qui agit seule, tandis que les offres de prêt frauduleuses annoncées en ligne sont l'œuvre de groupes organisés. Des réseaux criminels d'Afrique occidentale utilisent maintenant Internet pour repérer d'éventuelles victimes au Canada par l'intermédiaire de sites Web de publicité ou de vente aux enchères, et communiquent avec elles par courriel.

Selon les plaintes documentées par le CAAC, les sommes envoyées par les victimes en réponse à une sollicitation frauduleuse varient de 3,99 \$ à plus de 1 M\$. Les arnaques aux tirages et aux loteries sollicitant de faibles montants d'argent par la poste (de 3,99 \$ à 29,99 \$) servent généralement à dresser des listes de victimes à cibler pour l'obtention de sommes plus élevées.

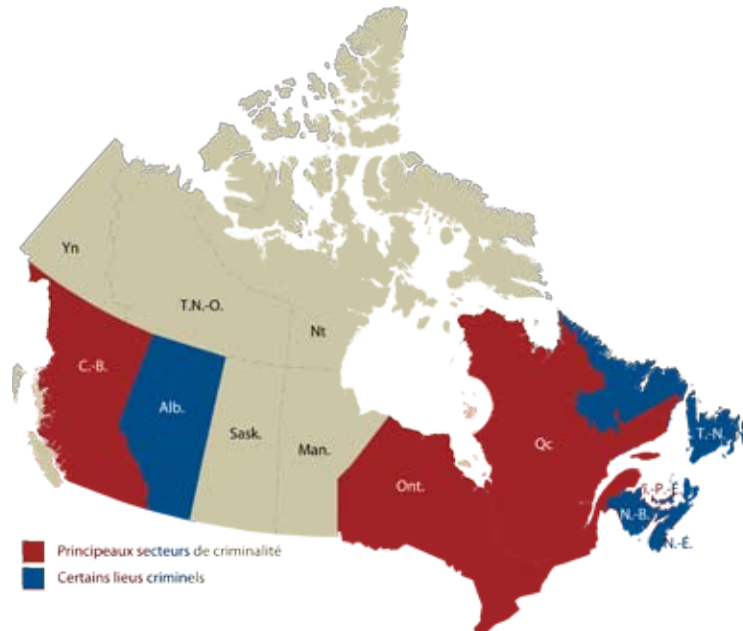
Certains stratagèmes visent à obtenir des sommes allant de 199 \$ à 499 \$ mais ciblent un nombre plus élevé de consommateurs. Les montants demandés dans le cadre de combines de prix ou de type 419 peuvent varier selon la relation établie entre la victime ciblée et le fraudeur.

Principaux foyers de FMM au Canada

Les lieux où des activités de FMM ont été signalées se situent principalement au Québec, en Ontario et en Colombie-Britannique. De telles activités ont aussi été signalées en Alberta, et certaines présenteraient des liens avec les provinces de l'Atlantique.

Un examen des rapports du CAAC révèle que les stratagèmes d'origine canadienne ciblent principalement des Américains. Les efforts de répression au Canada ont grandement contribué au repérage des foyers de FMM au Canada, notamment à Toronto, Vancouver et Montréal. Bien que les arnaques relevées aient surtout ciblé des Canadiens et des Américains, des plaintes ont été reçues de plus de 25 pays. Aucune tendance marquée n'a toutefois été dégagée à cet égard¹³.

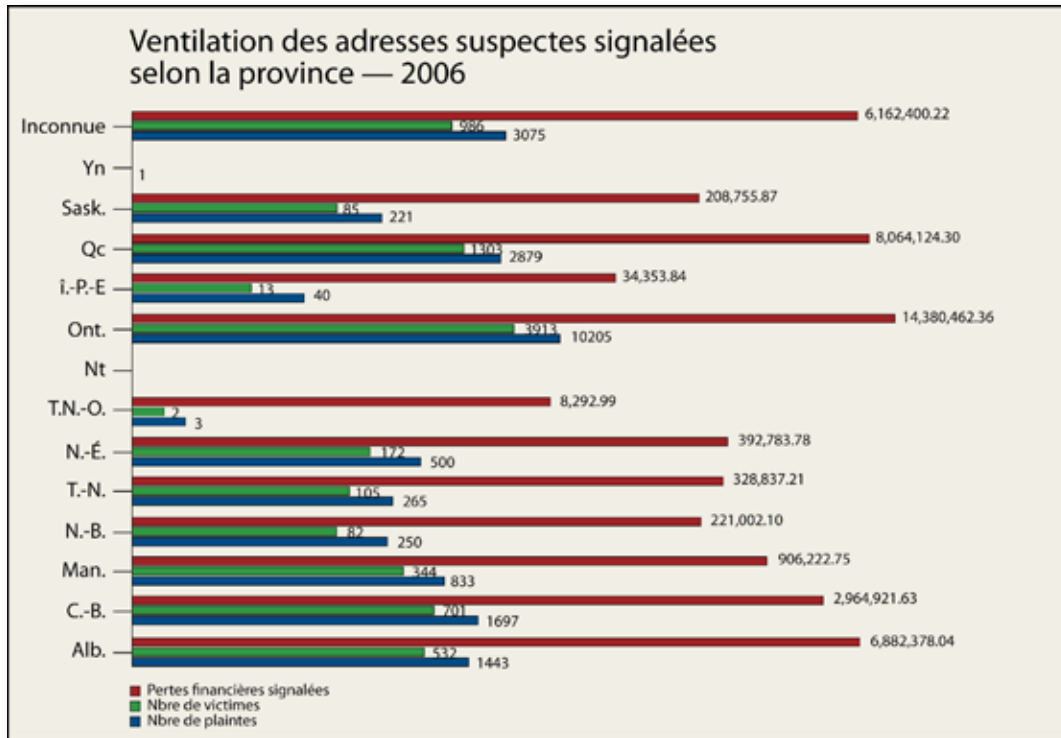
Ces escroqueries tirent également profit des nouvelles méthodes de communication, telles que les systèmes VoIP et les cellulaires prépayés. L'utilisation de cellulaires ne date pas d'hier, mais les fraudeurs en marketing de masse recourent de plus en plus au service prépayé, ce qui leur offre une mobilité accrue, de sorte qu'ils peuvent exercer leurs activités à partir de n'importe où, avec l'indicatif régional et le numéro de téléphone de leur choix. Il est alors difficile pour la police de déterminer l'identité des fraudeurs et leur lieu d'activité.



Secteurs criminels signalés

13 Voir le tableau à l'annexe B.

Graphique 8

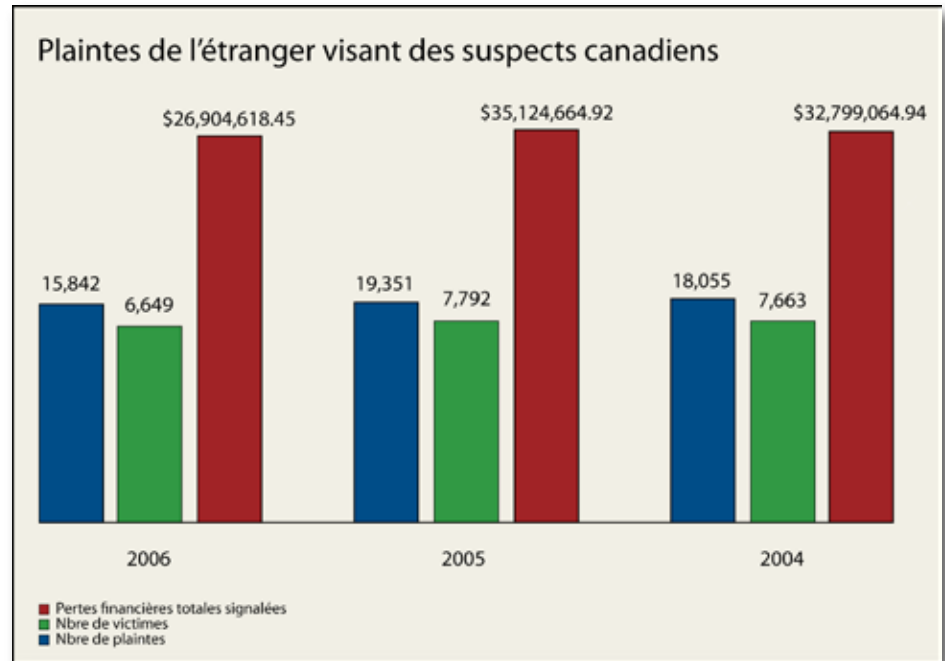


D'après les chiffres présentés ci-dessus, l'Ontario, le Québec, la Colombie-Britannique et l'Alberta seraient les principaux foyers de FMM au Canada. Près de la moitié des lieux signalés étaient en Ontario¹⁴.

En 2006, 73,9 % des plaintes reçues par le CAAC relativement à des suspects canadiens venaient de consommateurs dans des pays étrangers. L'analyse des appels reçus sur la ligne sans frais du CAAC indique que 37 % de ces appels viennent des États-Unis.

14 Il n'a pas été possible d'obtenir des chiffres pour 2004 et 2005.

Graphique 9



Caractéristiques des activités exercées selon la région

Bien que Toronto, Montréal et Vancouver demeurent les trois principaux foyers de FMM, les activités de ce genre ont connu une hausse dans d'autres villes canadiennes aussi, notamment Calgary, Winnipeg, Regina et Ottawa. L'utilisation de chèques contrefaits par des réseaux criminels ouest-africains pour exécuter des stratagèmes de FMM et les activités de répression des groupes policiers intégrés ciblant la FMM dans les grands centres urbains expliquent peut-être la dispersion des activités de FMM.

Les arnaques aux loteries, aux tirages, aux subventions, aux prêts et aux cartes de crédit s'exercent partout. Les combines liées aux répertoires et aux fournitures de bureau sont basées surtout à Montréal et, dans quelques cas, à Toronto.

Montréal (Québec)

Principales arnaques ayant fait l'objet d'enquêtes dans le cadre du Projet COLT à Montréal :

- les combines de *loterie* ou de *prix* qui ciblent principalement des Américains et certains Canadiens;
- les stratagèmes de *subvention gouvernementale* et de *prêt* qui ciblent des Américains seulement;
- l'arnaque de la *trousse médicale* qui cible certains Américains mais surtout des Canadiens (dans bien des cas, les fraudeurs se font passer pour des représentants de Santé Canada et ciblent des entreprises canadiennes);
- les escroqueries liées à des *programmes médicaux* qui consistent en la vente trompeuse de médicaments et qui ciblent des victimes américaines seulement; les offres de rabais sur l'achat de médicaments moyennant des frais de 300 \$ ciblant des victimes canadiennes.

La plupart des locaux de vente sous pression à Montréal se trouvent au centre-ville. La plupart sur l'île de Montréal ciblent des victimes anglophones, surtout américaines et canadiennes, selon le stratagème employé.

Les arnaques aux prix (loteries et tirages) sont exécutées principalement par téléphone et entraînent des pertes financières plus élevées par victime. Les pertes individuelles liées à ce genre d'escroquerie peuvent varier de 3 000 \$ à 100 000 \$. Les combines de loterie ou de tirage se prêtent mieux aux poursuites en vertu du *Code criminel* que d'autres types d'escroquerie, en grande partie parce que les loteries et les prix en question sont entièrement fictifs. Dans la plupart de ces cas, la nature frauduleuse du stratagème ne fait aucun doute. La majorité de ces arnaques (environ 95 %) ciblent des aînés.

Les combines de subvention, de prêt et de redressement de crédit entraînent des pertes financières moins élevées, mais touchent davantage de victimes. La plupart des personnes ciblées ont une faible cote de solvabilité. Lors du Projet CORAL¹⁵, on a relevé un grand nombre de victimes américaines, dont les pertes s'élevaient en moyenne à 300 \$US par personne.

Les fraudeurs qui exploitent des stratagèmes de subvention, de prêt, de redressement de crédit, de trousse médicale, de répertoire, de fournitures de bureau ou de produits anti-télémarketing essaient souvent de donner l'apparence d'une entreprise légitime.

De plus en plus d'opérations international de répression visent des fraudes utilisant de chèques contrefaits.

Toronto (Ontario)

Des arnaques de prêt, de carte de crédit à faible taux d'intérêt, de répertoire, de prix et d'ordre médical ont été relevées et ont fait l'objet d'enquêtes dans la grande région de Toronto.

Les offres de prêt frauduleuses visent généralement des consommateurs américains au moyen de petites annonces publiées dans des journaux, mais on constate maintenant l'utilisation d'Internet pour créer des sites Web faisant la promotion de fausses compagnies de prêt, ce qui a fait grimper le nombre de victimes à l'extérieur des États-Unis.

Comme l'arnaque aux subventions gouvernementales découverte à Montréal, les stratagèmes de carte de crédit à faible taux d'intérêt et d'ordre médical ciblent souvent exclusivement des consommateurs américains dont la cote de solvabilité laisse à désirer.

On assiste par ailleurs à la prolifération des arnaques de FMM axées sur l'utilisation d'instruments financiers contrefaits ou modifiés. Bien que la plupart des activités de ce genre aient été associées à des réseaux criminels ouest-africains, les renseignements dont on dispose actuellement portent à croire que ces groupes ne sont pas les seuls en cause. Par exemple, le CAAC a reçu des plaintes relatives à des offres d'emploi frauduleuses exigeant que le candidat soit un agent financier.

Les renseignements recueillis à ce jour indiquent aussi que certaines combines de prix ayant fait l'objet d'enquêtes à Toronto ciblent des résidents des États-Unis et du Royaume-Uni par téléphone et misent parfois sur la poste pour cibler des consommateurs américains.

Vancouver (Colombie-Britannique)

En Colombie-Britannique, les enquêtes ont surtout porté sur des combines de loterie ciblant des consommateurs aux États-Unis et au Royaume-Uni. Les listes de prospection sont établies à la suite de sollicitations postales invitant les destinataires à participer à une loterie ou à un tirage. Certains des stratagèmes qui ont fait l'objet d'enquêtes ont aussi été reliés à des réseaux criminels internationaux et à l'usage d'instruments financiers contrefaits ou modifiés. Les fonds envoyés par les victimes sont souvent encaissés à l'aide d'employés corrompus de comptoirs de services de transfert de fonds, et les produits de la fraude sont recyclés au moyen de comptes à l'étranger. Certaines des activités découvertes en Colombie-Britannique ont été associées à des combines de FMM exploitées dans d'autres provinces.

15 Projet Coral – voir le résumé de cas à la partie G sous la rubrique « Répression ».

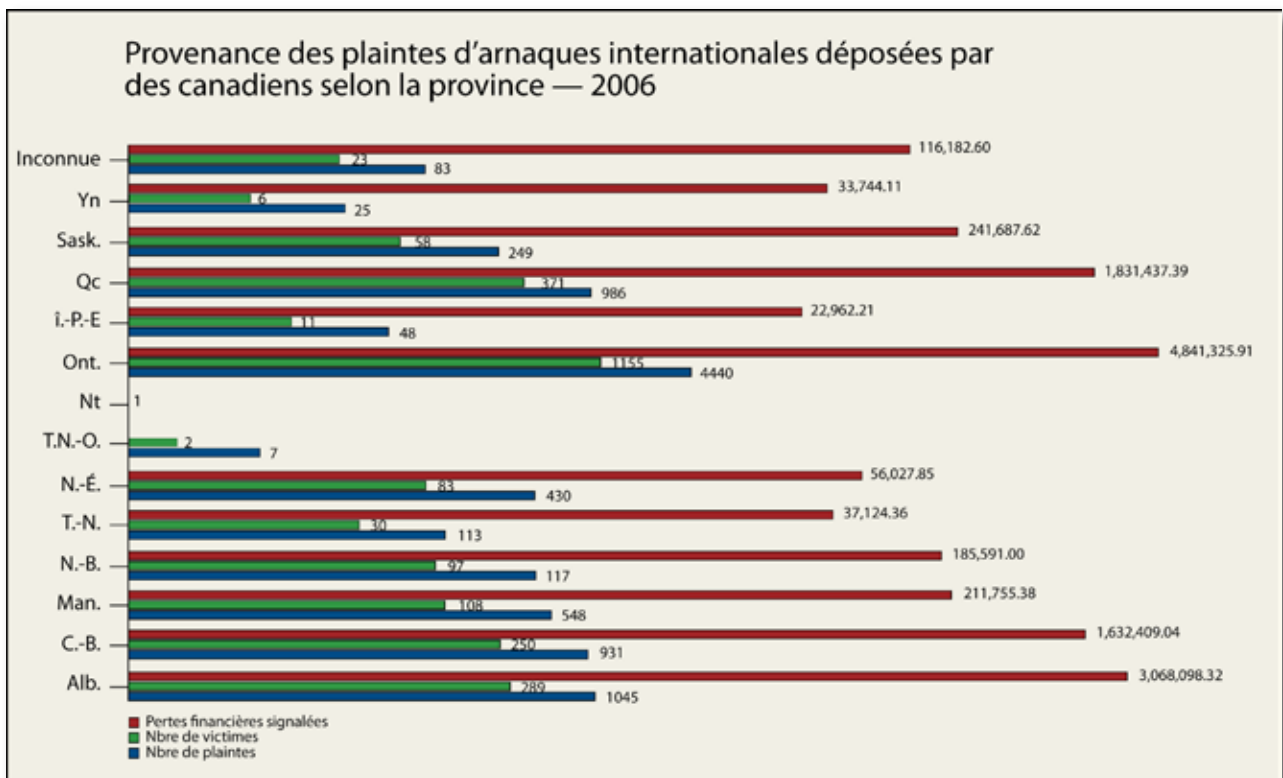
Fraudes d'origine étrangère ciblant des Canadiens

Comme on l'a déjà mentionné, les arnaques de FMM prennent une envergure de plus en plus internationale et les escrocs ne font pas de discrimination parmi les cibles possibles.

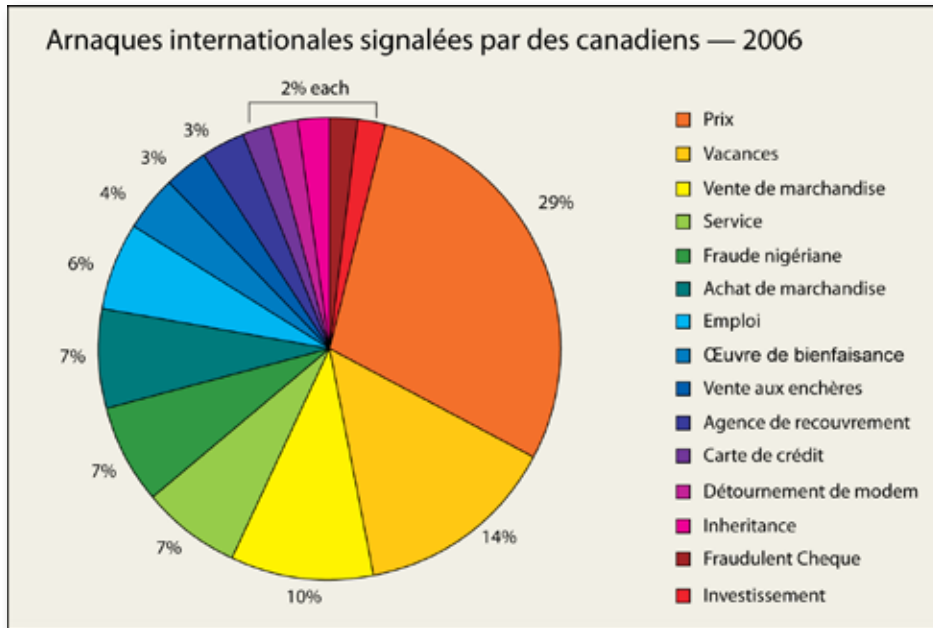
Les moyens de communication tels que le courrier électronique, les systèmes VoIP et le réseau Internet en général facilitent les contacts entre les criminels et leurs cibles. De plus, ces moyens de communication sont relativement peu coûteux comparativement aux gains financiers que peuvent rapporter les arnaques. En 2006, le CAAC a documenté plus de 12 M\$ en pertes signalées par des Canadiens victimes d'escroqueries internationales.

En 2006, 62,63 % des plaintes signalées par des Canadiens au CAAC concernaient une sollicitation en provenance d'un pays étranger. Cela confirme la portée internationale de la menace que présente la FMM.

Graphique 10



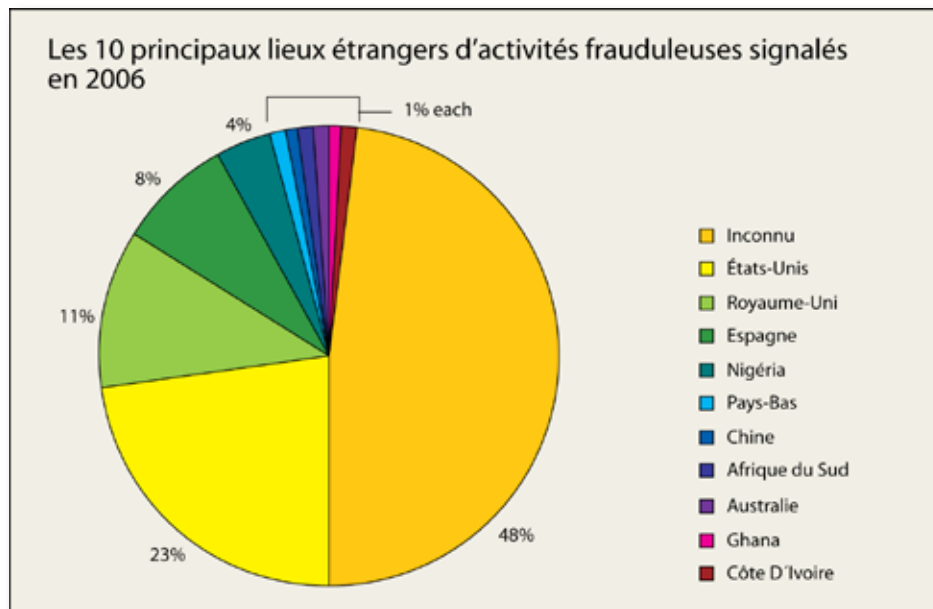
Graphique 11



Comparativement aux arnaques d'origine canadienne ciblant des Canadiens, les stratagèmes internationaux qui font des victimes au Canada visent davantage les particuliers que les entreprises. Deux des cinq principales combines d'origine canadienne ciblant des Canadiens qui ont été découvertes en 2006 visaient de façon particulière les entreprises; il s'agit des arnaques aux répertoires et aux fournitures de bureau.

En 2006, le CAAC a reçu 9 333 plaintes de la part de Canadiens qui signalaient des adresses suspectes à l'extérieur du Canada; 5 230 plaintes visaient des adresses suspectes dans 105 pays différents.

Graphique 12



Encore une fois, il convient de noter que les lieux d'activités de FMM se fondent sur les adresses suspectes signalées par des consommateurs et que ces adresses ne correspondent pas toujours au véritable endroit où se trouve le suspect.

Différences dans la fréquence d'activités criminelles déterminées

À l'heure actuelle, la tendance la plus marquée au chapitre de la FMM est le recours aux instruments financiers contrefaits ou modifiés pour faciliter l'exécution des stratagèmes. De mars à avril 2007, près de 30 % des plaintes reçues par le CAAC concernaient l'utilisation d'un instrument financier contrefait ou modifié.

L'utilisation de tels instruments donne un air de légitimité aux stratagèmes de FMM, puisque les escrocs ne demandent pas aux consommateurs d'envoyer leur propre argent, mais plutôt d'encaisser un instrument financier contrefait ou modifié et de retourner ensuite les frais exigés. C'est pratique courante dans les combines de prix, de prêt, d'emploi et de paiement excédentaire.

Les arnaques documentées qui misent sur l'utilisation de faux chèques ont une ampleur mondiale. Dans le cadre de ces stratagèmes, on passe de plus en plus par des comptes bancaires étrangère pour le recyclage des produits de la fraude. Le CAAC a documenté l'existence de tels comptes en Afrique du Sud, en Chine, au Costa Rica, aux Émirats arabes unis, au Ghana, à Hong Kong, au Japon, en Corée, à Singapour, au Nigéria, au Royaume-Uni, aux États-Unis, en Irlande, en Italie et en Espagne.

Les arnaques aux cartes de crédit et aux subventions gouvernementales sont facilitées au moyen d'adresses postales aux États-Unis et ciblent presque exclusivement des consommateurs américains. Elles sont encore exploitées à partir de locaux traditionnels de vente sous pression, dont la plupart ont été ou sont dotés de systèmes VoIP.

Certains réseaux de FMM se distinguent par leur taille, par leur degré de complexité et par la nature de leurs activités. Les activités de FMM peuvent aussi être exercées par une personne seule, ce qui a moins de chances d'attirer l'attention qu'une entreprise dotée de plusieurs employés traitant un volume élevé de transactions.

Pour ce qui est du type de stratagème employé, les différences tiennent parfois à la méthodologie appliquée. Par exemple, les arnaques aux loteries sont relativement peu coûteuses à gérer et visent à soutirer de fortes sommes aux victimes, tandis que les combines aux subventions gouvernementales et aux cartes de crédits impliquent des coûts plus élevés (bureaux), ciblent un public plus vaste et misent sur la sollicitation de sommes relativement faibles.

D. TYPES D'ORGANISATIONS ET DE GROUPES CRIMINELS

Locaux traditionnels de vente sous pression

Au Canada, les activités de FMM sont exercées tant par des individus que par des groupes organisés. La structure des locaux traditionnels de vente sous pression comprend habituellement le ou les propriétaires, les gestionnaires et les télévendeurs. Ces entreprises ont souvent besoin de services spécialisés, ce qui les amène à faire appel à des facilitateurs.

Profil changeant des fraudeurs en marketing de masse

Dans une étude publiée en 2002, le département de sociologie de l'Université du Tennessee a présenté les résultats d'entrevues avec plusieurs personnes reconnues coupables de télémarketing frauduleux. La description de leur profil révèle que la plupart venaient de la classe moyenne et qu'elles n'avaient habituellement aucun antécédent criminel.

Depuis, on a constaté une évolution de ce profil à la lumière d'enquêtes récentes. Les partenariats et les groupes d'intervention qui oeuvrent dans le domaine de la FMM au Canada ont découvert que des organisations criminelles participaient directement ou indirectement à la FMM. On croit que ce virage pourrait être attribuable entre autres au fait que les activités de FMM offrent un fort potentiel lucratif moyennant des risques et des coûts relativement faibles. Selon les renseignements recueillis dans le cadre d'enquêtes sur le sujet, certains groupes utiliseraient les profits ainsi réalisés pour financer leurs autres activités criminelles, dont le trafic de drogues et d'armes à feu.

Réseaux criminels Internationale

Au Canada, les données d'enquête et de renseignement indiquent que des cellules de réseaux criminels internationale se sont établies ou ont pris de l'ampleur dans diverses régions du pays. Ces réseaux ont diversifié leurs activités frauduleuses en délaissant les arnaques aux lettres de type 419 au profit, notamment, de combines de loterie, de paiement excédentaire, d'offre d'emploi et de fraude par groupe d'affinité. Ils utilisent couramment des instruments financiers contrefaits, surtout de faux chèques, à l'appui de leurs sollicitations frauduleuses.

Certaines cellules entretiennent des relations internationales avec d'autres réseaux pour faciliter l'exécution des stratagèmes. Différents membres du réseau s'occupent de différents aspects d'une arnaque. Rien n'indique que les cellules ou les réseaux soient organisés selon une hiérarchie déterminée, mais les membres des cellules se spécialisent dans différents aspects des combines. Par exemple, certains s'occupent de la sollicitation d'éventuelles victimes par courriel, d'autres se chargent des communications téléphoniques avec ces dernières, et d'autres encore postent les chèques aux personnes ciblées.



Difficultés inhérentes au repérage des groupes fraudeurs

En général, les réseaux frauduleux en marketing de masse ont une portée internationale et ont mis au point des stratégies pour échapper au droit pénal grâce à l'utilisation de téléphones cellulaires prépayés et de comptes de courrier électronique publics. Leur structure fluide complique d'autant plus l'identification des personnes impliquées. Plus longtemps ces personnes travaillent au sein d'un tel réseau, plus elles perfectionnent leurs compétences et les moyens qu'elles emploient relativement à différents aspects des combines de frais anticipés.

Certains stratagèmes utilisés au Canada sont conçus pour donner une impression de légalité et de légitimité au consommateur en lui fournissant des produits ou des services, bien que ceux-ci n'aient jamais été commandés ou demandés ou ne soient pas conformes aux promesses données. Comme les arnaques de ce genre sont généralement exploitées ouvertement sous forme d'entreprises de façade, elles sont relativement faciles à repérer pour les organismes d'application de la loi. Dans cette catégorie, on trouve notamment les combines aux subventions gouvernementales et aux répertoires. D'autres stratagèmes fonctionnent de manière plus subversive et emploient des tactiques plus directes. Les adeptes de ces stratagèmes ne fournissent rien en échange de l'argent versé par le consommateur et exercent leurs activités dans la clandestinité pour éviter d'être repérés. C'est notamment le cas des arnaques aux prix et aux prêts.

L'utilisation d'Internet, de systèmes VoIP, de cellulaires prépayés et de centres d'appels tiers permet aux groupes criminels d'échapper aux autorités policières canadiennes. Grâce à Internet et à la technologie VoIP, les fraudeurs peuvent dissimuler leur lieu d'activité réel. De même, ils privilégient les cellulaires prépayés puisqu'ils peuvent utiliser des renseignements frauduleux pour en faire la demande.

Les centres d'appel tiers permettent aux fraudeurs de fournir aux victimes des coordonnées autres que les leurs. Ils leur permettent également de rester au courant des vérifications faites par la police ou des plaintes déposées.

Sources de financement

Comme on l'a déjà expliqué, certaines activités frauduleuses exigent peu de ressources et d'infrastructures, tandis que d'autres peuvent nécessiter des infrastructures plus complexes et coûteuses.

Plusieurs stratagèmes internationaux de FMM exigent très peu de ressources et d'infrastructures. On n'a qu'à penser aux milliers d'escrocs installés dans des cybercafés un peu partout dans le monde, y compris en Afrique occidentale, en Europe et en Amérique du Nord. Souvent, tout ce qu'il faut, c'est une connexion Internet et un service postal.

Bon nombre des fraudeurs qui se dotent d'infrastructures plus complexes et coûteuses travaillent depuis plusieurs années dans le milieu plus traditionnel des locaux de vente sous pression. On croit que ces escrocs financent leurs nouvelles activités de FMM à l'aide des gains tirés de leurs fraudes antérieures.

E. PRINCIPALES TECHNIQUES DE FRAUDE

Recours à des facilitateurs

Certains intervenants peuvent, sciemment ou non, faciliter diverses étapes d'une activité frauduleuse, y compris son organisation initiale, le repérage d'éventuelles victimes, la prise de contact et les communications avec ces dernières, ainsi que la réception et le recyclage des fonds obtenus frauduleusement. Les facilitateurs varient selon la taille et la complexité du groupe en cause. Il est connu que les fraudeurs en marketing de masse au Canada ont recours aux intervenants suivants pour faciliter leurs activités :

Organisation initiale et logistique

Certains stratagèmes exigent l'aide de fournisseurs de services pour équiper des bureaux de services de télécopie, de téléphonie (système VoIP ou lignes traditionnelle) et d'accès Internet. Certains fraudeurs n'utilisent pas de bureau mais exercent leurs activités de manière plus souple au moyen de cellulaires prépayés, de sorte qu'ils peuvent se réunir dans des chambres d'hôtel ou des résidences, voire travailler à partir de leur véhicule.

Selon le stratagème employé et son degré de complexité, il peut être nécessaire de faire appel à plusieurs personnes pour l'exercice des activités, par exemple des télévendeurs, des coursiers et des gestionnaires. Ces personnes sont souvent recrutées au moyen d'offres d'emploi publiées dans des journaux, sur Internet et dans des campus collégiaux ou universitaires.

Certains arnaqueurs utilisent des centres d'appel tiers pour la prestation de services à la clientèle afin de se distancier encore davantage de leurs activités. La plupart de ces centres d'appel se trouvent au Canada, mais ils peuvent aussi être situés à l'étranger, par exemple en Inde. Les arnaques aux prix et aux loteries sont toutes exécutées au moyen de cellulaires prépayés.

Repérage d'éventuelles victimes

Le ciblage des victimes se fait en fonction de la méthode de communication choisie et du stratagème employé. Certaines fraudes, comme les lettres d'Afrique occidentale (fraudes 419), sont commises à l'aide d'extracteurs de courriel qui parcourent Internet à la recherche des adresses électroniques de cibles possibles. Dans d'autres cas, notamment les arnaques liées à une loterie, à un tirage ou à une autre remise de prix, le fraudeur monte un kiosque dans un centre commercial ou une foire professionnelle. Autre méthode employée par les escrocs pour repérer des victimes : l'envoi postal de sollicitations relatives à une loterie, un tirage ou une consultation avec un voyant demandant au destinataire de répondre en fournissant des renseignements personnels. Les vendeurs de listes de prospection sont une autre ressource spécialisée qu'utilisent les télévendeurs pour le repérage de victimes. Les fraudeurs échangent ou vendent souvent entre eux les listes de prospection. Il arrive aussi que les arnaques soient simplement annoncées dans les médias (journaux, télévision, radio, pourriel, messages éclairs sur Internet ou sites Web) afin de joindre d'éventuelles victimes.

Communication avec les victimes

La communication avec les victimes exige le recours à des fournisseurs de services de téléphonie, d'accès Internet et de courrier ou de messagerie.



Réception de l'argent envoyé par les victimes

Parmi les modes de paiement acceptés par les fraudeurs en marketing de masse, on note les services de transfert de fonds, les virements bancaires (y compris par courriel), les cartes de crédit, les chèques, l'argent comptant, les mandats, les traites bancaires et PayPal. En 2006, une analyse générale des plaintes de FMM déposées auprès du CAAC¹⁶ a dégagé les modes de paiement les plus couramment utilisés dans ce type de fraude, à savoir : Western Union (48 %), MoneyGram (18 %), les cartes de crédit (5 %), les chèques (3 %), les virements télégraphiques bancaires (2 %) et les retraits prélevés directement dans les comptes des victimes (2 %) (ex. : traitement par chambre de compensation automatisée).

Recyclage des produits de la fraude

Les fraudeurs en marketing de masse utilisent les mêmes techniques et les mêmes facilitateurs qui seraient employés pour n'importe quelle autre activité criminelle organisée (trafic de drogues et de produits de contrebande, jeu illégal, etc.). Par exemple, ils utilisent des noms de compagnies légitimes, des comptes bancaires à l'étranger, des prête-noms et des casinos. Ils font aussi appel à des courtiers pour convertir les espèces en marchandises aux fins de revente.

Méthodes de sollicitation et pertes financières connexes

Les stratagèmes de FMM sont souples; les fraudeurs qui en usent peuvent concevoir une sollicitation adaptée à n'importe quel produit, service ou événement.

Le télémarketing (appels directs) figure au premier rang des méthodes de sollicitation employées pour la FMM (y compris pour les combines de loterie, de tirage, de carte de crédit, de répertoire d'affaires, de fournitures de bureau, de subvention ou de prêt), tandis que les sollicitations en personne (arnaques aux placements) entraînent systématiquement les pertes financières les plus élevées. On a constaté une hausse considérable de l'utilisation des services postaux entre le Canada et d'autres pays, notamment les États-Unis, le Royaume-Uni et le Nigéria, pour faciliter la fraude transfrontalière, particulièrement dans le cadre de stratagèmes axés sur l'utilisation d'instruments financiers contrefaits (chèques et mandats), tels que les combines de loterie, de tirage, de paiement excédentaire et d'offre d'emploi.

Le tableau suivant fait état des pertes financières globales attribuables aux fraudes en marketing de masse d'origine canadienne visant des Canadiens, selon la méthode de sollicitation, pour les trois dernières années :

16 L'analyse n'a pas fourni une ventilation détaillée des principaux modes de paiement selon les types de FMM.

Tableau 6

Année	APPELS DIRECTS			POSTE			PRESSE ÉCRITE		
	Tentatives	Victimes	Pertes Financières Signalées	Tentatives	Victimes	Pertes Financières Signalées	Tentatives	Victimes	Pertes Financières Signalées
2006	2 677	468	1 268 009,78 \$	655	229	655 362,52 \$	118	192	513 645,16 \$
2005	3 158	586	1 612 003,05 \$	700	212	145 249,43 \$	115	164	393 414,99 \$
2004	3 319	499	2 781 080,59 \$	428	216	34 787,27 \$	189	189	431 978,18 \$
TOTAL	9 154	1 553	5 661 093,42 \$	1 783	657	835 399,22 \$	422	545	1 339 038,33 \$
Année	INTERNET / COURRIEL			TÉLÉCOPIEUR EN PERSONNE					
	Tentatives	Victimes	Pertes Financières Signalées	Tentatives	Victimes	Pertes Financières Signalées	Tentatives	Victimes	Pertes Financières Signalées
2006	350	421	858 066,51 \$	23	3	295 000,00 \$	92	199	9 419 999,12 \$
2005	282	492	1 054 323,78 \$	30	5	133 066,67 \$	137	220	3 139 333,70 \$
2004	283	321	930 964,37 \$	40	13	4 417,80 \$	148	147	1 189 849,89 \$
TOTAL	915	1 234	2 843 354,66 \$	93	21	432 484,47 \$	377	566	13 749 182,71 \$
Année	AUTRE/INCONNU			RENVOI			TÉLÉVISION/RADIO /MÉDIAS		
	Tentatives	Victimes	Pertes Financières Signalées	Tentatives	Victimes	Pertes Financières Signalées	Tentatives	Victimes	Pertes Financières Signalées
2006	148	79	561 754,96 \$	10	13	108 133,02 \$	11	9	2 130,97 \$
2005	183	163	2 570 983,62 \$	9	16	1 969 292,08 \$	9	11	748,84 \$
2004	167	140	1 791 416,09 \$	7	10	61 218,93 \$	3	13	8 702,72 \$
TOTAL	498	382	4 924 154,67 \$	26	39	2 138 644,03 \$	23	33	11 582,53 \$

De façon générale, au cours des trois dernières années, le télémarketing (appels directs) s'est classé au premier rang des méthodes de sollicitation selon le nombre de cas signalés. Viennent ensuite, dans l'ordre, les sollicitations par la poste, par Internet, dans la presse écrite et en personne. Du point de vue des pertes financières, les sollicitations en personne sont systématiquement les plus réussies, parce qu'elles sont commises par des « personnes de confiance », comme les appelle l'American Association of Retired Persons. D'après les documents de cette association, ces personnes jouissent d'un immense avantage, puisque leurs victimes les connaissent avant la perpétration du crime. Il peut s'agir d'un parent, d'un ami, d'un voisin, d'un nouvel amoureux, d'un soignant...¹⁷

Du point de vue du taux de victimes, les sollicitations en personne (60 %), par la poste (60 %), par Internet (57 %) et dans la presse écrite (56 %) sont les plus efficaces pour tromper les Canadiens. Selon l'analyse des données recueillies jusqu'à maintenant, il semble probable que les stratagèmes de télémarketing demeureront les principales méthodes de sollicitation signalées au CAAC et très probable que les arnaques par la poste et sur Internet continueront de prendre de l'ampleur en 2007.

17 http://www.aarp.org/research/international/speeches/june15_06_shurme.html

F. RÉCEPTION ET RECYCLAGE DES PRODUITS DE LA FMM



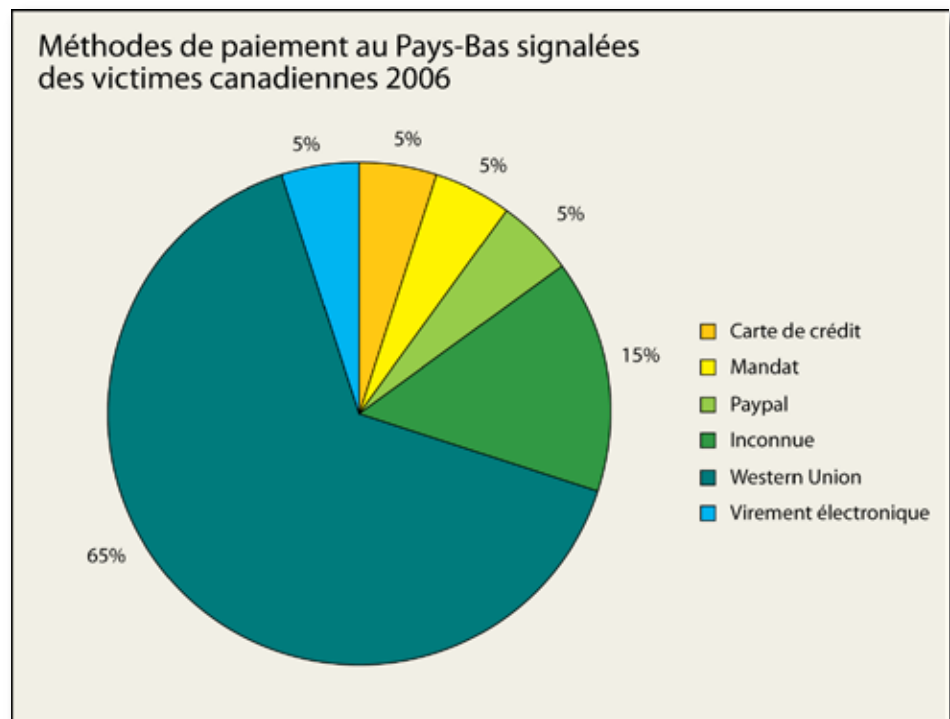
Principaux moyens de recevoir les fonds envoyés par les victimes

Par le passé, les fonds étaient acheminés au fraudeur par la poste sous forme de chèque ou d'argent comptant, mais de nouvelles méthodes sont maintenant employées à cette fin. Les services de transfert de fonds semblent de plus en plus prisés à cet égard.

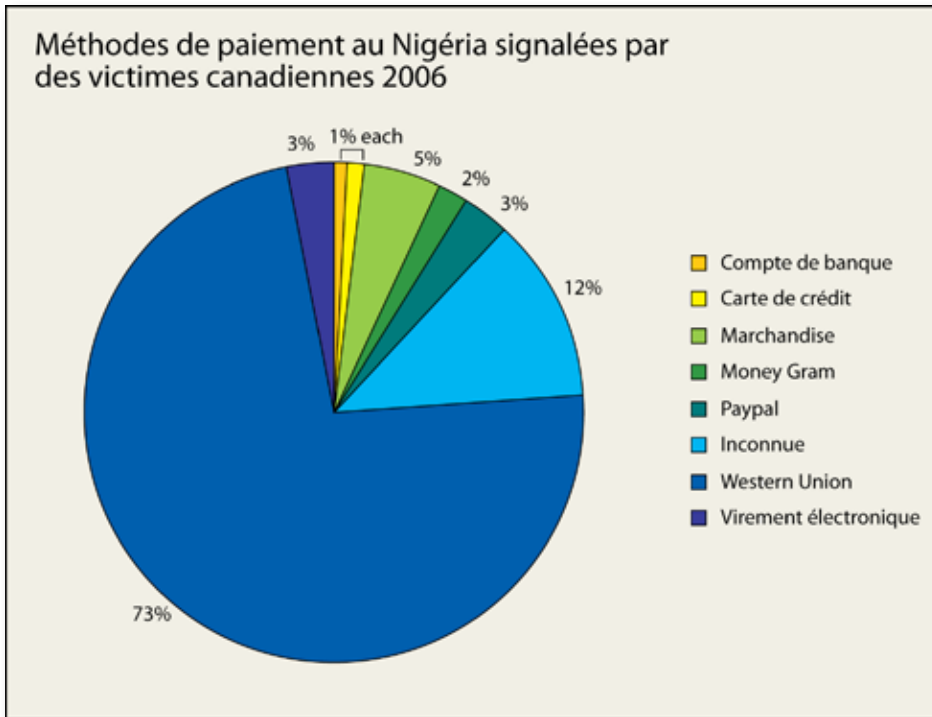
Avec plus de 250 000 et plus de 100 000 points de service dans le monde respectivement, ces compagnies offrent un réseau mondial d'agents situés notamment dans des dépanneurs, des épiceries, des agences de voyage, des services d'encaissement de chèques et des comptoirs de change. Pour recevoir des fonds obtenus frauduleusement dans ces points de service, les arnaqueurs ont recours soit à de fausses pièces d'identité, soit à un agent complice. Il suffit d'avoir le numéro de contrôle du virement pour prendre possession des fonds à presque n'importe quel point de service. Dans le cas des activités de fraude où Internet constitue le principal moyen de communication et de transaction, les paiements sont habituellement reçus par l'intermédiaire de services de paiement Internet tels que PayPal.

Les graphiques suivants illustrent les méthodes utilisées pour faire des paiements dans différents pays :

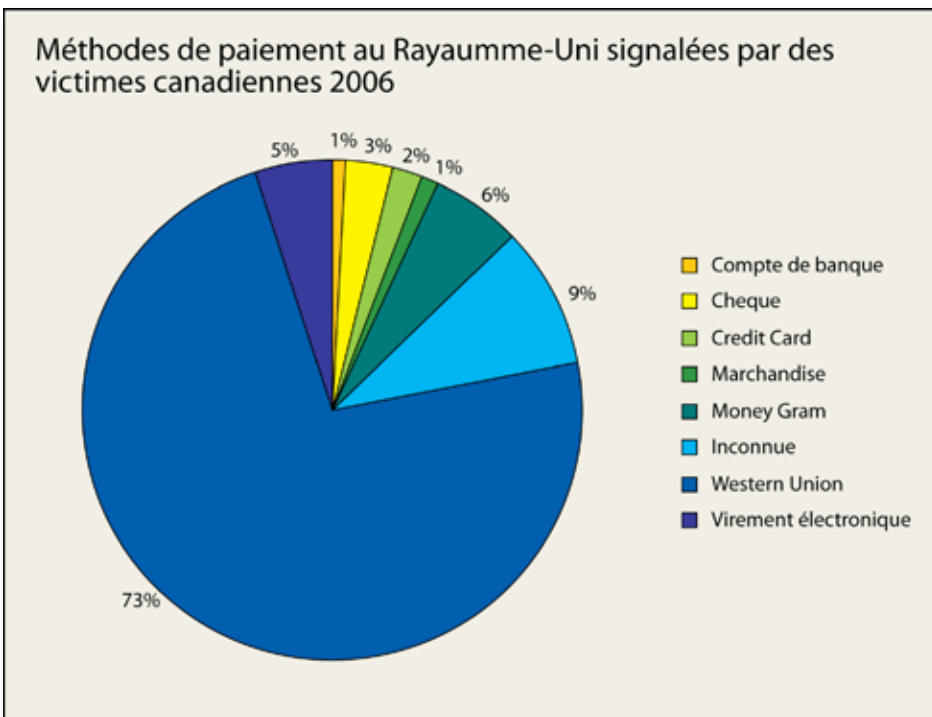
Graphique 13



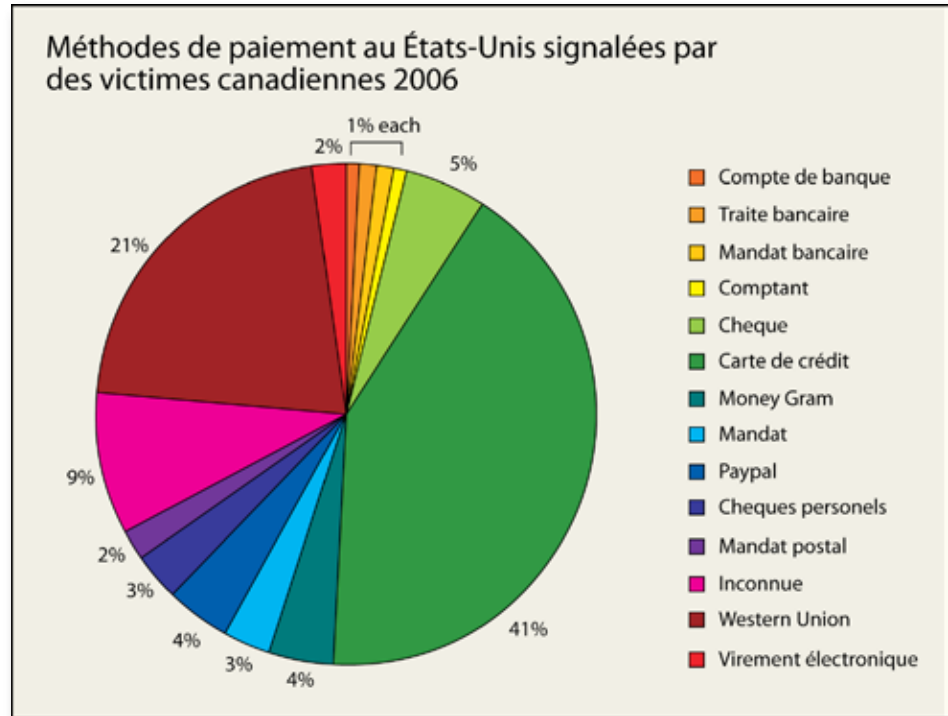
Graphique 14



Graphique 15



Graphique 16



Principaux moyens de recycler les fonds reçus des victimes

Les organisations criminelles exploiteront toute nouvelle occasion de blanchir les produits de leurs activités illicites. Parmi les méthodes en usage depuis un certain temps, mentionnons le « schtroumpfage »¹⁸, les virements de fonds électroniques, le recours à des entreprises de transfert de fonds ou de vente de titres négociables, les casinos, les cartes de crédit et le regroupement de fonds au moyen d'entreprises légitimes. On note aussi quelques tendances naissantes qui ont fait l'objet d'enquêtes récemment et qui revêtent un intérêt particulier pour le blanchiment de fonds tirés de la FMM : le recours aux services de paiement Internet, aux cartes de crédit prépayées et aux monnaies numériques.

Comme les produits de la FMM sont reçus par chèque, en espèces ou au moyen de services de paiement Internet, il faut les recycler afin d'établir une distance entre les fonds et l'activité criminelle initiale. Contrairement aux chèques, qui doivent être déposés dans un compte bancaire pour permettre d'autres virements électroniques afin de brouiller les pistes, l'argent comptant peut facilement être introduit dans les systèmes financiers par d'autres moyens. Les cartes de crédit prépayées et les monnaies numériques sont de plus en plus utilisées dans le processus de blanchiment puisqu'elles offrent plusieurs avantages intéressants aux fraudeurs, dont l'anonymat, l'aspect comptant, une portée internationale et des possibilités de virement partout dans le monde.

¹⁸ Technique de recyclage d'argent consistant à faire des dépôts inférieurs au seuil de déclaration en utilisant plusieurs comptes répartis dans des banques différentes.

Services de paiement Internet

Ce qui fait l'unicité des services de paiement Internet, c'est qu'ils permettent de transférer des fonds partout dans le monde sans passer par les voies bancaires habituelles. Essentiellement, deux utilisateurs inscrits à un service de paiement Internet peuvent transférer de l'argent entre leurs comptes d'un simple clic, à très peu de frais. Pour alimenter un tel compte, il faut normalement effectuer un télévirement à partir d'un compte bancaire. On peut également rattacher une carte de crédit au compte pour régler des achats au moyen du service de paiement Internet. Il existe trois façons de retirer des fonds d'un service de paiement Internet : par télévirement à un compte bancaire, par l'achat de marchandises dans un magasin virtuel ou en faisant un retrait à un guichet automatique avec une carte de débit ou de crédit.

Les services de paiement Internet ouvrent certainement la porte au recyclage d'argent. Ils peuvent servir d'outil dans le processus de blanchiment, surtout à l'étape de la dispersion, où les fonds peuvent être envoyés dans différents pays, et à celle du placement, comme instrument pour la réception des produits de la criminalité dans un compte. Ainsi, le fraudeur évite de rester pris avec une forte somme qui devra transiter par la banque. Il s'agit là d'une caractéristique particulièrement intéressante pour les activités de FMM commises sur Internet¹⁹.

Il y aurait moyen d'élaborer des stratagèmes complexes misant sur plusieurs virements de fonds dans différents pays où le fraudeur détient des comptes bancaires. L'argent serait alors transféré du compte de paiement Internet aux comptes bancaires. D'autres télévirements pourraient ensuite être faits, ou des traites bancaires pourraient être tirées sur ces comptes pour déplacer de nouveau les produits de la fraude.

Certains services de paiement Internet contrôlent les activités « suspectes », de sorte que les transferts de sommes importantes effectués sans raison précise de nature commerciale ou autre soulèveront probablement des questions ou seront bloqués si le détenteur du compte ne peut fournir une explication satisfaisante. Toutefois, l'utilisation de commerces de façade pour envoyer de fausses factures à des clients dans des pays étrangers pourrait permettre de contourner ce contrôle et de transférer de fortes sommes partout dans le monde.

Monnaies numériques

La monnaie virtuelle est une forme d'argent électronique émise par des sociétés privées. Le secteur du cyberargent est composé d'émetteurs de monnaie virtuelle et d'agents de change qui collaborent étroitement afin de permettre à leurs clients d'effectuer des opérations financières au moyen d'argent électronique. L'émetteur de la monnaie virtuelle en garantit habituellement la valeur sous forme d'or et d'autres métaux précieux et offre des services financiers (comptes chèques, télévirements, etc.) semblables à ceux des institutions financières ordinaires. Pour acheter ces devises numériques, on peut utiliser différents modes de paiement : télévirements, mandats, espèces, or, chèques personnels ou autres monnaies virtuelles.

La principale difficulté que soulèvent les monnaies virtuelles, du point de vue du recyclage d'argent, tient au fait que les fonds deviennent impossibles à suivre après leur dépôt, puisque les réseaux de cyberargent sont exploités par des compagnies privées à l'extérieur du système financier. Il est donc possible d'envoyer des fonds virtuels n'importe où dans le monde sans laisser de trace écrite ni de documents financiers, puisque toutes les opérations sont traitées par l'intermédiaire d'un serveur privé appartenant à l'émetteur de la monnaie virtuelle ou à l'agent de change.

Certains de ces émetteurs de monnaie virtuelle et de ces agents de change offrent même des cartes de débit rattachées au compte d'argent électronique, ce qui permet au détenteur de la carte d'obtenir des devises locales, des services et des biens partout dans le monde, à partir de n'importe quel guichet automatique ou point de vente.

Cartes de crédit prépayées

Les cartes de crédit prépayées n'ont fait leur entrée sur le marché canadien que récemment. Ces cartes peuvent être rechargeables ou non. Pour comme il s'agit d'un marché relativement nouveau au Canada, il est difficile d'en évaluer l'importance, mais il ne serait pas déraisonnable de penser qu'il se chiffre à plusieurs milliards de dollars.

Ces cartes soulèvent plusieurs préoccupations en ce qui concerne le blanchiment d'argent. Tout d'abord, il y a le processus d'identification, qui semble se limiter à des renseignements de base. De plus, certains des numéros d'identification demandés (comme les numéros de passeports étrangers) sont difficiles à vérifier. Dans certains cas, on ne demande même pas la date de naissance.

19 Bien qu'on n'ait aucun exemple précis de cette pratique, ce qu'il faut retenir c'est l'intérêt et les possibilités d'exploitation que présente cette caractéristique pour un fraudeur.

Ces cartes sont considérées un peu comme de l'argent comptant. Bien que plusieurs possibilités de rechargement soient offertes aux clients, cette particularité pourrait devenir problématique, surtout si les limites sont significativement hautes.

Autre élément inquiétant : les mouvements transfrontaliers d'espèces. Les cartes de paiement ne sont pas définies comme des instruments financiers aux termes de la partie 2 de la *Loi sur le recyclage des produits de la criminalité et le financement des activités terroristes* (L.R.C. 2000, c. 17). D'autre part, les postes frontaliers ne sont pas équipés de lecteurs pour déterminer les sommes portées aux cartes. Les transferts entre cartes peuvent aussi créer des problèmes à cet égard. Par exemple, quelqu'un pourrait acheter deux cartes, en envoyer une aux États-Unis par la poste et transférer de l'argent de sa carte au Canada à sa carte aux États-Unis. Comme les deux cartes ont été achetées au Canada, il n'est pas nécessaire de déclarer le transfert, quel qu'en soit le montant, parce qu'il s'agit d'une opération intérieure selon les définitions établies. Toutes les cartes de crédit prépayées offrent l'accès aux guichets automatiques du monde entier, et les fonds ainsi obtenus sont dans la devise locale.

Le dernier aspect préoccupant des cartes prépayées tient à la possibilité de les charger de monnaie virtuelle. Comme on l'a déjà expliqué, le principal problème avec la monnaie électronique, du point de vue du recyclage d'argent, c'est que les fonds deviennent impossibles à suivre du moment qu'ils sont déposés, puisque les réseaux de cyberargent sont exploités par des compagnies privées à l'extérieur du système bancaire officiel. Les opérations effectuées en monnaie virtuelle sont traitées par l'intermédiaire de serveurs qui appartiennent à des compagnies privées.

Estimation du volume de recyclage des produits de la FMM

Plusieurs enquêtes menées au Canada révèlent que les activités de FMM peuvent générer des revenus substantiels en relativement peu de temps.

Par exemple, à Montréal, le Projet CORAL²⁰ a mis au jour une entreprise criminelle qui a généré plus de 30 M\$US en 18 mois.

Une enquête menée dans le cadre du Projet EMPTOR portait sur une arnaque dirigée par un couple britannico-colombien qui offrait une protection pour carte de crédit à des clients de Los Angeles et ailleurs aux États-Unis et qui a soutiré plus de 10 M\$ à des milliers de victimes.

Au Canada, aucune estimation claire ne donne une idée de l'ampleur et du volume du recyclage des produits de la FMM. Il est aussi difficile de dépister et de saisir les produits de la fraude parce que les arnaqueurs se divisent les profits en espèces.

Identification de passeurs de fonds et de contrôleurs

Il est clair, d'après l'information recueillie dans le cadre d'enquêtes et les plaintes déposées par le public, que les fraudeurs en marketing de masse utilisent couramment les dépôts de virement télégraphique pour les virements de fonds de moins de 10 000 \$. Quant aux sommes de 10 000 \$ et plus, les chèques de banque et les virements télégraphiques interbancaires sont les méthodes les plus répandues.

Les chèques de banque sont envoyés à des adresses postales utilisées dans ce but précis. Parfois, les fraudeurs paient quelqu'un pour utiliser son adresse postale. Il faut alors prouver que la personne était consciente de la fraude. Toutefois, la plupart des opérations sont effectuées par virement télégraphique. Pour les sommes plus importantes, les fraudeurs ont normalement recours à des virements interbancaires.

L'argent comptant est habituellement envoyé par courrier ou par la poste ordinaire. Le Programme d'interception²¹ est un moyen efficace de perturber ces envois. Les sommes envoyées par les victimes peuvent aller de 3 000 \$ à 100 000 \$.

Des enquêtes ont signalés que des coursiers se rendaient au casino pour retirer de fortes sommes d'argent, la limite à cet égard étant fixée à 25 000 \$ dans cet établissement. Il s'agit là d'une méthode que les fraudeurs emploient pour retirer des fonds des comptes qui servent à recevoir l'argent des victimes au moyen de virements interbancaires. Normalement, lorsqu'on fait un retrait à un guichet automatique ou dans un point de vente, une limite maximale est établie pour chaque transaction ou pour chaque journée (par exemple de 500 \$). Or, au casino, on peut retirer jusqu'à 25 000 \$.

Certaines activités de blanchiment de produits de la FMM sont facilitées au moyen de sociétés à dénomination numérique et d'opérations bancaires extraterritoriales. Les plaintes du CAAC ont identifiés des comptes de banque au Japon, le Royaume-Uni, Pays-Bas, Allemagne, États-Unis, Israël, et Nigéria.

20 Projet Coral – Voir le résumé de cas à la partie G, sous la rubrique « Répression ».

21 Programme d'interception – Voir le résumé de cas à la partie G, sous la rubrique « Répression ».

G. PRATIQUES EXEMPLAIRES EN VIGUEUR POUR RÉDUIRE LA FRÉQUENCE DE LA FMM

Le Groupe de travail national sur la FMM, présidé par le Bureau de la concurrence, l'OPP et la GRC, a élaboré une stratégie nationale pour *démanteler, perturber et neutraliser les réseaux de FMM basés au Canada*. Dans cette optique, le groupe de travail a établi trois objectifs fondamentaux : 1) accroître les risques et les coûts liés aux activités de FMM; 2) renforcer l'efficacité des mesures de répression; 3) réduire la vulnérabilité des victimes.

Pour atteindre ces objectifs fondamentaux, les partenaires et les intervenants doivent instaurer des mesures novatrices qui pourraient, avec le temps, devenir des pratiques exemplaires.

Renseignement

Le CAAC (anciennement appelé « PhoneBusters ») et le Centre de SDDE sont les principaux points de collecte de renseignements sur les plaintes de FMM. L'information ainsi obtenue est ensuite analysée par le Groupe d'analyse des renseignements du CAAC.

Lancé par l'OPP en 1993, le Projet PhoneBusters est reconnu comme la première initiative de centralisation et d'enregistrement des plaintes relatives au télémarketing frauduleux. Le mandat initial de PhoneBusters consistait à centraliser l'enregistrement des plaintes et les enquêtes sur les cas de télémarketing frauduleux en Ontario. Très tôt, il est devenu évident que les télévendeurs qui cherchaient à frauder les résidents de l'Ontario ne se trouvaient pas eux-mêmes en Ontario, mais au Québec, et qu'ils ne ciblaient pas exclusivement des consommateurs ontariens²².

Les criminels canadiens qui se livrent à la FMM ciblent des Canadiens, des Américains et des résidents d'autres pays. Ils profitent de la mondialisation et des nouvelles technologies pour commettre leurs actes frauduleux, misant sur les limites entre les territoires de compétence pour éviter d'être repérés. Ils emploient des méthodes de plus en plus complexes et perfectionnées pour commettre leurs forfaits, créant des obstacles toujours plus difficiles à surmonter pour les organismes d'application de la loi et réduisant considérablement leur risque d'être traduits en justice.

En 1997, il était généralement reconnu que la FMM n'était pas un phénomène exclusivement canadien. Les données recueillies par PhoneBusters se sont avérées utiles pour évaluer les effets de la fraude sur les Canadiens, ce qui a grandement amélioré la capacité des responsables du gouvernement et de l'application de la loi à prévenir la FMM, à la réduire et à réagir à la menace qu'elle représentait pour les consommateurs²³.

Maintenant connu sous le nom de Centre d'appel antifraude du Canada (CAAC), PhoneBusters joue un rôle fondamental dans la prévention de la FMM et dans la sensibilisation aux stratagèmes connexes. Il favorise aussi le renseignement à l'appui de l'application de la loi en recueillant les plaintes en la matière et les renseignements sur les victimes, en les analysant et en les diffusant aux services de police compétents.



²² <http://www.phonebusters.com/francais/aboutus.html>

²³ <http://www.phonebusters.com/francais/aboutus.html>

La GRC a par ailleurs lancé un système de signalement des cas de fraude sur Internet appelé Signalement en direct des délits économiques (SDDE) en 2003. Il s'agit d'un site protégé conçu pour accepter des plaintes de fraude venant de partout dans le monde, à condition qu'elles présentent un lien avec le Canada (par exemple une victime ou un suspect se trouvant au Canada). Lorsque les plaintes répondent à certains critères de priorité, le système de SDDE les communique automatiquement au service de police compétent. Le but ultime du SDDE est de favoriser l'échange de renseignements informatisé en temps réel entre les organismes d'application de la loi et de réglementation qui se penchent sur les plaintes de fraude provenant des consommateurs.

La centralisation des plaintes de fraude est essentielle pour améliorer l'échange de renseignements et favoriser la production de renseignements. La fusion prochaine des bases de données du CAAC et du SDDE permettra d'accepter toute plainte de fraude présentant un lien avec le Canada, qu'elle soit déposée par téléphone, par la poste, par télécopieur ou par Internet. Ainsi, n'importe quelle personne ou organisation, où qu'elle se trouve, pourra déposer une plainte ou échanger de l'information avec l'organisme d'application de la loi compétent.

Répression

Partenariats et groupes de travail

Au Canada, les six partenariats de lutte contre la FMM, qui comprennent trois groupes d'intervention mixtes, sont les principaux organes de répression chargés d'enquêter sur les activités de FMM, de les perturber et de démanteler les groupes qui en sont responsables.

Comme les activités de FMM se concentrent dans les grandes villes, à savoir Toronto, Montréal et Vancouver, les partenariats et les groupes d'intervention en la matière ont été établis dans ces régions. Même s'il s'agit d'une réponse ponctuelle à la FMM, chaque partenariat ou groupe d'intervention a établi des objectifs précis adaptés aux besoins des organismes qui en font partie. Ces opérations policières conjuguées doivent respecter le mandat de chaque organisme participant afin de maintenir un niveau d'engagement suffisant. Le succès de ces partenariats et groupes d'intervention a jeté les bases d'une répression continue et croissante de la FMM.

Projet COLT

Souvent considéré comme le premier groupe d'intervention au Canada, le Projet COLT a été établi officiellement en 1998 sous la direction de la GRC. Il s'agit d'une opération

policière conjuguée visant à combattre les activités de télémarketing frauduleux d'origine canadienne. En sont partenaires l'Immigration and Customs Enforcement (ICE) Bureau du U.S. Department of Homeland Security (DHS), la Sûreté du Québec (SQ), le Service de police de la Ville de Montréal (SPVM), le FBI, le Bureau de la concurrence Canada, la U.S. Federal Trade Commission (FTC) et le U.S. Postal Inspection Service (USPIS).

Le but du Projet COLT est de repérer les organisations qui usent de stratagèmes de télémarketing, d'enquêter sur leurs activités, de les perturber, d'en saisir les produits et de rembourser les victimes. Pour ce faire, il mise sur trois stratégies : l'enquête, l'interception et la prévention.

Points saillants des activités de répression du Projet COLT

De 2004 à 2006, les enquêteurs du Projet COLT ont reçu plus de 2 000 plaintes concernant des pertes de plus de 75 M\$ attribuables à la fraude par télémarketing.

En sa qualité de groupe d'intervention orienté par le renseignement, le Projet COLT entreprend des enquêtes de grande envergure qui visent à identifier et à cibler les échelons supérieurs des organisations criminelles qui se livrent à la FMM. Cette façon de procéder s'est avérée très efficace et a permis au groupe de constater que les réseaux de FMM pratiquent souvent plusieurs activités criminelles.

Les résumés suivants donnent un aperçu des enquêtes entreprises dans le cadre du Projet COLT et de la nature des activités de FMM au Québec :

Projet CORAL

Le Projet CORAL est une enquête qui a été menée en 2004 relativement à un réseau de FMM basé au Québec qui ciblait des Américains. L'enquête a été lancée par suite d'une demande d'entraide juridique de l'ICE du DHS. Au départ, le stratagème consistait à vendre des trousseaux de redressement de crédit, puis à offrir des subventions gouvernementales et des prêts. Chaque vente montait à environ 299 \$US. Environ 2,2 millions d'appels ont été faits sur une période de six mois. Le réseau comptait un certain nombre de locaux de vente sous pression, dont certains étaient dotés de systèmes VoIP. Il a donc fallu obtenir de l'aide technique pour démanteler les systèmes informatiques et téléphoniques. Un employé corrompu dans une banque américaine se chargeait de transférer les fonds soutirés aux victimes. On estime qu'en 17 mois, le groupe a réalisé des gains bruts de 30 M\$.

Projet CASINO

Le Projet CASINO a été lancé en 2003 pour enquêter sur un réseau international de télémarketing frauduleux, qui employait un stratagème de frais anticipés et de loterie. Les victimes se trouvaient aux États-Unis et au Royaume-Uni, et certaines d'entre elles ont perdu jusqu'à 100 000 \$US. Sept suspects ont été arrêtés à Montréal et inculpés aux États-Unis.

Alliance stratégique de Toronto

L'Alliance stratégique de Toronto a été établie en 2000 dans le cadre d'une vaste initiative entreprise par les gouvernements des États-Unis et du Canada pour améliorer la collaboration entre les deux pays dans la lutte contre la fraude. En sont membres la FTC des États-Unis, le USPIS, l'escouade des fraudes du Service de police de Toronto, le ministère des Services gouvernementaux de l'Ontario, la Direction de la lutte contre l'escroquerie de l'OPP, le Bureau de la concurrence Canada, la GRC et l'Office of Fair Trading du Royaume-Uni.

Points saillants des activités de répression de l'Alliance stratégique de Toronto :

Bien qu'il n'ait pas été possible d'obtenir le nombre exact de dossiers ouverts de 2004 à 2006, l'Alliance a parvenu des informations sur un grand nombre de dossiers importants. L'Alliance souligne que, malgré l'absence de données précises, l'Alliance estime que les chiffres fournis sont prudents et inférieurs aux pertes totales réelles²⁴.

Trois dossiers pour la période de 2004 à 2006, portaient sur des stratagèmes qui auraient touché plus de 500 000 victimes et généré plus de 200 M\$ en ventes nettes. L'Alliance stratégique de Toronto se concentre sur le repérage rapide et le démantèlement des groupes de FMM. En misant sur des renseignements tactiques et opérationnels pour repérer les groupes de FMM et sur le CAAC et le Consumer Sentinel pour obtenir de l'information sur les plaintes et les victimes, l'Alliance a réussi à éliminer les sollicitations liées aux cartes de crédit dans la région du Grand Toronto. Elle coordonne ses enquêtes avec tous ses partenaires afin de permettre le dépôt d'accusations en vertu du *Code criminel* et de la *Loi sur la concurrence*, l'engagement de poursuites au civil par la FTC et l'éventuelle extradition des sujets aux États-Unis.

Les résumés de cas suivants illustrent la complexité et la portée des stratagèmes basés dans la région du Grand Toronto :

Projet CENTURION

Il s'agit d'une enquête menée en 2005 sur une combine de télémarketing consistant à offrir des cartes de crédit à des consommateurs américains moyennant des frais initiaux de 249 \$. Lorsqu'un consommateur acceptait cette offre, son compte bancaire était débité par un tiers, mais au lieu de recevoir une carte de crédit, il recevait des formulaires de demande de cartes à valeur stockée.

C'est dans le cadre de cette enquête que l'Alliance a fermé son plus grand local de vente sous pression, où travaillaient plus de 150 employés. On estime que le groupe en question aurait fraudé plus de 120 000 victimes et recueilli 35 M\$. Les locaux de vente sous pression visés par l'enquête étaient tous équipés de systèmes VoIP, et il a fallu obtenir de l'aide technique pour démanteler l'équipement informatique et téléphonique qui s'y trouvait.

Projet SPIN MARKETING

Cette enquête menée en 2005 portait sur une arnaque de loterie ciblant des Américains. L'arnaque se déroulait en deux étapes. Dans un premier temps, on disait aux consommateurs qu'ils avaient gagné une loterie mais qu'ils devaient d'abord payer des frais par carte de crédit, chèque ou mandat pour avoir accès à leur prix. Au cours de la deuxième étape, on ciblait des aînés pour essayer de les amener à se cotiser à plusieurs pour acheter des billets de loterie. Quelques billets étaient alors achetés et photocopiés pour convaincre les victimes de la légitimité de leur participation.

Autres dossiers notables :

Une combine de fausse facturation relative à des fournitures de bureau et à des services de publicité dirigée sous le nom de Trader's International a ciblé des entreprises dans plus de 25 pays.

Le Projet IMPACT, une initiative du Groupe d'intervention contre les bandes criminalisées et les armes à feu du Service de police de Toronto, a identifié des stratagèmes de prêts offerts par télémarketing à des consommateurs américains.

24 *The Toronto Strategic Partnership*, janvier 2007

Projet EMPTOR

Il s'agit d'un groupe d'intervention multi organismes dirigé par la GRC et mis sur pied en 1998 pour enquêter sur le télémarketing illégal. En sont partenaires la Business Practices and Consumer Protection Authority (BPCPA) de la Colombie-Britannique, le Bureau de la concurrence Canada, la FTC des États-Unis, le USPIS et le FBI.

Ce projet vise à repérer et à perturber les réseaux de télémarketing de haut niveau basés en Colombie-Britannique par la saisie de biens et le dépôt d'accusations au criminel. Il mise sur une intervention à trois volets : enquête, interception et éducation.

Un élément qui est propre à l'équipe du Projet EMPTOR est la possibilité d'invoquer des lois provinciales (notamment la *Business Practices and Consumer Protection Act*) contre les FMM. De plus, l'équipe utilise des traités d'entraide juridique pour faciliter l'arrestation et l'extradition des fraudeurs en marketing de masse. Le résumé de cas suivant est un exemple d'un stratagème de FMM découvert en Colombie-Britannique :

EUROBOND

Cette enquête a été amorcée en 2004 par suite de renseignements reçus d'un ancien employé du principal suspect. Selon ces renseignements, le stratagème employé consistait à téléphoner à des personnes aux États-Unis pour leur offrir des bons d'épargne d'autres pays. On disait également aux éventuelles victimes que l'achat d'un bon d'épargne les rendrait admissibles à un prix. Mille de victimes identifiées a entraîné des pertes de 3 M\$US.

Partenariat de l'Alberta contre la fraude transfrontalière

En vigueur depuis 2003, le Partenariat de l'Alberta contre la fraude transfrontalière est un regroupement binational d'organismes d'application de la loi qui collaborent afin de repérer, de prévenir, de combattre, de juguler et d'enquêter sur les pratiques de vente trompeuses et les activités criminelles frauduleuses exercées à partir de l'Alberta ou touchant cette province. En sont membres Services Alberta, le Service de police de Calgary, le Bureau de la concurrence, le Service de police d'Edmonton, la GRC, la FTC des États-Unis et le USPIS.

De 2005 à 2006, le Partenariat a enquêté les arnaques de prix, des offres de carte de crédit, des opérations pyramidales, des offres de répertoire, des offres d'emploi et des combines liées à Ebay. Le résumé de cas suivant fait ressortir certaines des caractéristiques de la FMM en Alberta.

Centurion Financial

Avec l'assistance du CAAC, le Partenariat a découvert un local de vente sous pression où l'on communiquait avec des consommateurs américains pour leur proposer une carte de crédit moyennant des frais initiaux. Les activités de ce local étaient directement liées à l'enquête Centurion à Toronto. Le groupe en cause utilisait un système VoIP et passait par un agent tiers pour débiter les comptes des victimes.

Alliance stratégique de Vancouver

L'Alliance stratégique de Vancouver a été formée en 2004 à titre d'initiative mixte du Bureau de la concurrence, du Service de police de Vancouver, de la BPCPA, du USPIS et de la FTC des États-Unis. L'Office of Fair Trading du Royaume-Uni a aussi entrepris des démarches pour se joindre à l'Alliance. Ce partenariat vise à repérer les activités de télémarketing frauduleux basées dans la région de Vancouver, à les perturber, à mener les enquêtes connexes et à poursuivre les personnes responsables.

Partenariat de l'Atlantique — Combattons la fraude transfrontalière

Ce partenariat établi en 2005 vise à repérer les pratiques commerciales trompeuses et les activités criminelles frauduleuses exercées à partir de la région de l'Atlantique et ciblant des consommateurs américains ou exercées à partir des États-Unis et ciblant des résidents du Canada atlantique; à mener les enquêtes connexes; à poursuivre les personnes responsables et, ainsi, à réduire ces pratiques et activités. En font partie la GRC, la Société canadienne des postes, le Service de police de Charlottetown, le Bureau de la concurrence Canada, la police régionale de Halifax, le bureau du procureur général du Nouveau-Brunswick, la Force constabulaire de Terre-Neuve, le Service de police de Saint John, Service Nova Scotia and Municipal Relations, la FTC des États-Unis et le USPIS.

En 2006, le Partenariat a ouvert deux dossiers de FMM concernant un répertoire en direct et une arnaque de prix misant sur l'utilisation de chèques contrefaits.

Sommaire des données d'enquête

Les dossiers examinés révèlent que, au cours des trois dernières années, les enquêtes menées au Canada ont ciblé des stratagèmes concernant des prix, des prêts, des subventions gouvernementales, des cartes de crédit, des répertoires, le domaine de la santé et des offres de placement. La plupart des enquêtes gérées par les partenariats et les groupes d'intervention concernent des fraudes transfrontalières entre le Canada et les États-Unis, dont certaines visent des victimes dans les deux pays. Aucune enquête n'a porté

sur des victimes canadiennes ciblées exclusivement par des fraudeurs en marketing de masse établis au Canada ou par des arnaques dirigées à partir d'autres pays.

Perturbation

Programme d'interception :

Le Programme d'interception est une stratégie efficace pour la perturbation des activités transfrontalières de FMM. Il s'agit d'intercepter à leur arrivée au Canada les paiements en espèces et les effets négociables envoyés aux fraudeurs par des victimes aux États-Unis ou ailleurs. La GRC continue d'encourager la participation de partenaires clés au Programme, dont l'Agence des services frontaliers du Canada (ASFC) et les services postaux et de messagerie. Chaque année, des millions de dollars sont ainsi interceptés et retournés aux victimes.

Les projets COLT et EMPTOR sont des groupes d'intervention multi organismes basés à Montréal et à Vancouver respectivement, qui luttent contre les activités de FMM sous la direction de la Section des infractions commerciales de la GRC. Depuis la création des groupes d'intervention en matière de FMM, l'ASFC a joué un rôle de premier plan dans les efforts concertés pour freiner la FMM. L'ASFC a contribué activement à l'interception de fortes sommes d'argent venant de l'extérieur du Canada, surtout de la part d'âinés aux États-Unis ou au Royaume-Uni qui avaient été bernés par des fraudeurs canadiens en marketing de masse.

En 2004, grâce au Programme d'interception, l'équipe du Projet EMPTOR a intercepté et retourné aux victimes environ 865 000 \$ en espèces et en effets négociables. Elle a également intercepté des chèques contrefaits totalisant 14,2 M\$ destinés à des victimes aux États-Unis. Au moins une partie de ces chèques auraient été encaissés par les victimes. En 2005, l'équipe du Projet EMPTOR a intercepté environ 1 M\$ en espèces et en effets négociables et 118 M\$ en chèques contrefaits. Depuis 1998, avec l'aide de l'ASFC, l'équipe du Projet COLT a intercepté 5 884 305 \$ qui auraient été empochés par des criminels sans son intervention. L'appui de l'ASFC a contribué de façon importante à prévenir des fraudes et à retourner l'argent aux victimes. Le Programme d'interception est très apprécié des organismes partenaires aux États-Unis.

Tous les cas d'interception et de récupération ont nécessité une collaboration absolue entre le secteur privé (service télégraphique) et les organismes de réglementation et de police, tant au Canada qu'aux États-Unis.

Programme de visites sur place

Le Programme de visites sur place est une des activités de perturbation exercées par l'équipe d'interception et de prévention du Projet COLT à Montréal. Au moins une fois par mois, l'équipe au complet du Projet COLT fait des visites auprès de locaux de vente sous pression dans la région de Montréal. Les locaux ciblés sont choisis à partir de renseignements transmis par le CAAC ou de plaintes reçues directement du public.

Le Programme a pour objectif d'amener ces locaux à fermer leurs portes ou à tout le moins de perturber leurs activités par suite d'une visite de la police.

Pour obtenir des résultats optimaux, on coordonne les visites sur place avec les partenaires du Projet COLT : la GRC, la SQ, le SPVM, le Bureau de la concurrence, le FBI, l'ICE du DHS, la FTC et le USPIS. L'Agence du revenu du Canada (ARC) participe également à ces activités.

Prévention et éducation

Le Forum canadien sur la prévention de la fraude

Mars est le mois de la prévention de la fraude au Canada et partout dans le monde. C'est l'occasion pour les membres du Forum sur la prévention de la fraude (FPF) d'accroître la sensibilisation aux dangers de la fraude et d'éduquer le public en fonction de sa devise : « *Identifiez-la. Signalez-la. Enrayez-la.* » Le Forum est présidé par le Bureau de la concurrence et regroupe des entreprises du secteur privé, des groupes de consommateurs et de bénévoles ainsi que des organismes gouvernementaux et policiers qui se préoccupent de la fraude ciblant les particuliers et les entreprises et qui sont résolus à la combattre. Il connaît chaque année une croissance presque exponentielle à mesure qu'y adhèrent de nouveaux organismes policiers, gouvernementaux et du secteur privé.

SeniorBusters

En 1999, PhoneBusters a mis sur pied SeniorBusters, un programme de volontariat qui regroupe maintenant une soixantaine de membres bénévoles âgés de plus de 50 ans. Essentiellement, ce programme vise à stimuler la discussion entre aînés, étant donné la vulnérabilité particulière de ce groupe démographique aux escroqueries. Les bénévoles viennent de milieux divers et apportent toutes sortes de compétences au programme pour essayer de réduire le télémarketing frauduleux ciblant les aînés. SeniorBusters peut communiquer avec les familles de victimes, avec les services de police compétents et avec des comités de lutte contre la maltraitance des aînés. Il fournit aux aînés les outils dont ils ont besoin pour éviter de devenir des victimes de fraude.

CONCLUSION



La FMM demeure un problème au Canada et cause de graves préjudices à ses victimes, non seulement ici, mais aussi à l'étranger. Les activités de FMM qui s'exercent au Canada peuvent être simples ou complexes et ont souvent une portée internationale. Elles ont des répercussions financières sur les Canadiens et peuvent ébranler la confiance des consommateurs.

Les criminels perçoivent la FMM comme une activité très lucrative à faible risque. En effet, cette forme de criminalité présente un ratio risques-avantages complètement déséquilibré. Aux yeux des fraudeurs en marketing de masse, les gains possibles liés à la perpétration de telles fraudes au Canada l'emportent largement sur les risques infimes de détection et de poursuite. La FMM demeure donc une avenue extrêmement intéressante.

Tandis que les activités de FMM se poursuivent au Canada, des pratiques semblables prennent de l'ampleur dans d'autres pays. Les facteurs suivants peuvent jouer dans l'expansion et la mondialisation de la FMM:

- Bien que les fraudeurs en marketing de masse continuent d'utiliser couramment le téléphone et la poste, Internet a permis aux criminels d'élargir leur bassin de victimes et de prendre contact avec des cibles presque partout dans le monde, à très peu de frais.
- Les fraudeurs peuvent maintenant se procurer logiciels, matériel informatique et imprimantes à des prix abordables afin de contrefaire des instruments financiers.
- Grâce aux nouveaux moyens de télécommunications, les criminels peuvent exercer leurs activités dans la clandestinité, presque n'importe où.
- Les paiements électroniques, les virements bancaires télégraphiques et les comptoirs de paiement en espèces permettent aux fraudeurs d'exercer leurs activités sans égard aux frontières lorsqu'il s'agit de recevoir les fonds envoyés par les victimes et de recycler les produits de la fraude.

Les arnaques aux frais anticipés d'origine étrangère demeurent un problème. Elles ont évolué au point où bon nombre d'entre elles misent sur l'utilisation de faux chèques. Les réseaux criminels internationaux sont les principaux auteurs des escroqueries nationales ou internationales de ce genre. En règle générale, ces réseaux ont une portée internationale et ont mis au point des stratégies qui compliquent les enquêtes criminelles par l'utilisation de téléphones cellulaires prépayés et de comptes de courriel publics. La structure et la continuité de ces réseaux leur donne de la stabilité et leur permet de se spécialiser dans plusieurs aspects des combines de frais anticipés et de raffiner les techniques qu'ils emploient.

Nouvelle tendance la distribution massive de faux chèques sous le couvert d'entreprises légitimes. Selon ce genre de stratagème, les fraudeurs persuadent les victimes d'encaisser un chèque et de leur retourner une partie des fonds.

Les activités de FMM découvertes au Canada étaient basées surtout en Ontario, au Québec, en Colombie-Britannique et en Alberta. Dans les secteurs plus peuplés, le nombre de victimes est plus élevé. D'après les données sur les plaintes recueillies par le CAAC et le Centre de SDDE, c'est en Ontario que les activités de FMM et le nombre de victimes sont les plus importants.

Les stratagèmes de FMM employés au Canada ne ciblent pas uniquement des Canadiens. Certains groupes ont établi des réseaux internationaux pour faciliter la réception des fonds envoyés par les victimes, comme dans le cas des réseaux criminels d'Afrique occidentale qui utilisent des comptes bancaires en Asie.

Les dossiers examinés révèlent que, au cours des trois dernières années, les enquêtes policières au Canada ont ciblé des combines de prix, de prêt, de subvention gouvernementale, de carte de crédit, de répertoire, de services de santé et de placement.

La plupart des enquêtes menées par les partenariats et les groupes d'intervention établis ont visé des fraudes transfrontalières entre les États-Unis et le Canada. Certains de ces dossiers concernaient des victimes dans les deux pays. Aucun ne portait sur des victimes canadiennes ciblées exclusivement par des fraudeurs en marketing de masse basés au Canada ou par des arnaques dirigées à partir d'autres pays.

Au cours des trois dernières années, on n'a obtenu aucun renseignement permettant de déterminer le nombre d'activités de FMM au Canada.

Les données d'enquête examinées ne permettaient ni de dégager des tendances en matière de blanchiment d'argent ni de déterminer la destination ultime des produits de la FMM.

L'information recueillie dans le cadre des enquêtes menées au cours des trois dernières années ne permet pas de déterminer s'il y a des activités de FMM au Canada qui touchent uniquement des Canadiens. La portée de la FMM est internationale, et tous les partenariats et les groupes d'intervention établis comprennent une présence américaine.

Les données d'enquête recueillies jusqu'à maintenant permettent uniquement de connaître le nombre d'arrestations, les types d'arnaques, les pertes financières qui y sont associées et le nombre de personnes qui en sont victimes. À défaut de faire un sondage auprès des organismes de police et de réglementation qui donnent suite aux incidents de FMM, la collecte de données d'enquête présente des lacunes.

Le télémarketing (appels directs) est la méthode de sollicitation la plus signalée pour les combines de FMM, tandis que les contacts en personne donnent systématiquement lieu aux pertes les plus élevées. Le recours aux services postaux pour faciliter la fraude transfrontalière entre le Canada et les États-Unis a connu une hausse substantielle.

L'analyse comparative des 12 arnaques les plus courantes établit une base pour la détermination des activités et des tendances en FMM qui présentent la plus grande menace pour le Canada. Les cinq combines en tête de liste sont, dans l'ordre, les offres de prix (y compris les loteries et les tirages frauduleux), les offres d'emploi ou de travail à la maison, les offres d'argent en provenance de l'étranger (combines de type 419), les offres de prêt et les combines de paiement excédentaire (vente de marchandises). Tous ces stratagèmes ont été associés à l'utilisation d'instruments financiers contrefaits ou modifiés et ont une portée internationale.

Pour leur part, les partenaires canadiens reconnaissent qu'ils ne sont pas aussi bien équipés et organisés qu'ils pourraient l'être pour combattre efficacement le problème de la FMM au Canada. Ils saisissent parfaitement l'importance d'éliminer l'aspect profitable des activités de FMM et d'en équilibrer le ratio risques-avantages par l'instauration d'une série de mesures conçues pour perturber, démanteler et neutraliser les groupes canadiens qui s'y livrent.

Les partenariats et les groupes d'intervention ont collaboré à certains dossiers mais ils ne coordonnent pas activement au plan national les enquêtes ciblant les activités et les tendances en FMM. Tous les dossiers examinés portaient sur des suspects canadiens qui ciblaient des consommateurs américains, et tous exigeaient une coordination et une collaboration transfrontalières entre les autorités policières du Canada et des États-Unis.

La stratégie mise au point par le Groupe de travail national sur la FMM est en voie de redéfinir le mode d'intervention canadien, et les travaux en cours relativement aux différents piliers de cette stratégie élargiront le bassin de connaissances de tous les intervenants concernés.

Les enquêtes menées par les partenariats et les groupes d'intervention montrent que la FMM est organisée et que ses auteurs ont de fortes chances d'être associés à plusieurs activités criminelles, telles que le recyclage d'argent, le narcotrafic, la contrefaçon et les infractions liées aux armes. On soupçonne fortement que les produits de ces activités de FMM ont servi à financer d'autres activités criminelles.

Certains groupes de FMM ont la capacité d'infiltrer l'économie légitime et d'utiliser des entreprises légitimes pour faciliter les aspects de leurs stratagèmes qui ont trait aux communications et aux produits de la fraude.

La FMM est une forme de criminalité qui exige une intervention collaborative de la part des organismes d'application de la loi et de réglementation, du gouvernement et du secteur privé. Les groupes d'intervention et les partenariats établis connaissent énormément de succès dans leurs enquêtes en matière de FMM, mais ils disposent de ressources limitées.



ANNEXES

ANNEXE — A

Les 12 principales arnaques signalées par des Canadiens en 2006

(Au 14 mars 2007)

Afin d'établir une liste plus juste des types de FMM les plus signalés par les Canadiens, un groupe d'experts en la matière a entrepris une analyse comparative des listes des 10 combines de FMM les plus répandues dressées par PhoneBusters, le Centre de SDDE et le Bureau de la concurrence, tout en tenant compte des listes établies par le Bureau d'éthique commerciale et le Consumer Sentinel. Le groupe a également établi des définitions pratiques utilisables par les divers intervenants concernés au Canada.

1- Offre de prix/loterie/tirage : Toute sollicitation fausse ou trompeuse informant les victimes qu'elles ont gagné ou qu'elles courent la chance de gagner quelque chose à condition d'acheter d'abord un produit ou de payer des frais initiaux tels que des taxes. (Par exemple : Vous avez gagné une voiture! Mais pour la réclamer, vous devez d'abord payer des frais.)

2- Possibilité de travail à la maison/d'emploi : Toute sollicitation fausse ou trompeuse proposant un emploi et demandant le versement de frais initiaux pour garantir l'emploi ou obtenir le matériel nécessaire pour faire le travail; toute offre d'emploi impliquant le transfert ou le virement télégraphique de fonds après encaissement d'instruments financiers.

3- Offre d'argent en provenance de l'étranger : Sollicitations traditionnellement appelées « fraude nigériane », « fraude 419 » ou « fraude d'Afrique occidentale » consistant généralement à offrir ou à demander de l'aide pour le transfert d'une forte somme d'argent d'un pays étranger au pays de la victime. Celle-ci doit payer des frais initiaux pour diverses raisons (taxes, frais de traitement, certificat antiterroriste, nettoyage de billets noircis, etc.) avant d'accéder au magot. Or, le magot est fictif et la victime ne reçoit jamais l'argent promis.

4- Offre de prêt : Toute sollicitation fausse ou trompeuse consistant à faire paraître une annonce dans une publication telle qu'un journal ou un magazine ou sur Internet afin d'offrir un prêt sans égard aux antécédents de crédit du consommateur. La victime répond à l'annonce et doit payer des frais initiaux pour avoir droit au prêt, qu'elle ne recevra jamais.

5- Combine de paiement excédentaire (vente de marchandise par le plaignant) : Tout incident où un consommateur vend une marchandise ou un service et reçoit du suspect un paiement sous forme d'instrument financier contrefait ou modifié (chèque, mandat, etc.) pour un montant supérieur au prix de vente. Le fraudeur demande ensuite à la victime d'encaisser le chèque et de lui retourner le montant excédentaire. Au bout du compte, le consommateur doit rembourser de sa poche le montant excédentaire envoyé après l'encaissement du chèque et peut perdre la marchandise si elle a déjà été expédiée.

6- Offre de répertoire d'affaires : Vente de répertoires spécialisés (sur papier, CD-ROM ou Internet) à des entreprises et à des organismes à but non lucratif au moyen de techniques trompeuses, dont celle de la « vente présumée ». Selon cette technique, les télévendeurs usent de réfutations et de dialogues préparés à l'avance et se font passer pour des services de recouvrement ou de vérification pour « conclure » une vente qui



n'a jamais eu lieu. Ils emploient ensuite divers scénarios pour faire croire aux organisations ciblées qu'elles ont des obligations contractuelles envers le groupe de télémarketing frauduleux.

7- Vente de fournitures de bureau : Toute sollicitation fausse ou trompeuse effectuée au moyen de tactiques de vente présumée, où la compagnie suspecte se fait passer pour l'habituel fournisseur de la victime, souvent en confirmant son adresse et en faisant mine d'offrir le produit à rabais ou à titre d'essai gratuit. Au moment de recevoir la facture, la victime voit que le produit est surfacturé et ne vient pas de son fournisseur habituel. Souvent, la compagnie suspecte refuse d'accepter le retour du produit ou exige des frais de restockage. Dans certains cas, la victime reçoit les fournitures et commence à les utiliser. Après les avoir utilisées en partie ou en totalité, elle reçoit une facture indiquant un prix supérieur à celui qu'elle aurait normalement payé à son fournisseur habituel.

8- Offre de vacances/de voyage : Toute sollicitation fausse ou trompeuse où il faut payer des frais initiaux pour réserver ou garantir un voyage. Souvent, on néglige de mentionner des renseignements importants et on offre un cadeau gratuit ou une récompense à la victime pour la convaincre d'assister à une présentation de vente où elle fera l'objet de fortes pressions ou recevra des renseignements trompeurs.

9- Produits ou services médicaux trompeurs : Toute promotion ou sollicitation fausse ou trompeuse ayant trait à des produits ou à des services médicaux tels que des remèdes ou des traitements, où les affirmations ne peuvent pas être vérifiées et où les consommateurs reçoivent des produits ou des traitements qui ne fonctionnent pas comme promis ou pas du tout. Par exemple : remèdes ou traitements contre le cancer, le vieillissement et les problèmes de santé mentale.

10- Achat de marchandises (articles non reçus ou non conformes) : La victime reçoit une facture ou fait un paiement relativement à des marchandises qui n'ont pas été commandées ou reçues. Il s'agit souvent de situations où le consommateur achète des produits sur Internet, par catalogue ou par la poste, mais ne les reçoit jamais.

11- Offre de carte de crédit : Toute sollicitation fausse ou trompeuse consistant à offrir une carte de crédit à un consommateur moyennant des frais initiaux. La victime paie les frais mais ne reçoit jamais la carte.

12- Offre de placement : Toute sollicitation fausse ou trompeuse concernant des possibilités de placement qui offrent souvent un rendement supérieur à la normale. Le consommateur perd la plupart ou la totalité de l'argent censément investi.

ANNEXE — B

STRATAGÈMES CANADIENS CIBLANT D'AUTRES PAYS - 2006

Plaintes concernant des pertes financières signalées au CAAC par des victimes à l'étranger

Pays du plaignant	TÉLÉMARKETING (TÉLÉPHONE)			COURRIER / PRESSE ÉCRITE			INTERNET / COURRIEL		
	Tentatives	Victimes	Pertes financières signalées	Tentatives	Victimes	Pertes financières signalées	Tentatives	Victimes	Pertes financières signalées
États-Unis	6 443	5 165	18 858 536,08 \$	1 893	566	1 683 746,99 \$	206	437	875 116,05 \$
Australie	0	1	168 467,00 \$	4	0	0,00 \$	0	2	40,94 \$
Royaume-Uni	8	18	154 847,03 \$	6	1	50,00 \$	0	5	413,86 \$
Allemagne	0	1	64 000,00 \$	0	0	0,00 \$	0	2	5 662,63 \$
France	0	2	32 485,00 \$	0	0	0,00 \$	1	0	0,00 \$
Suède	0	1	20 278,00 \$	0	0	0,00 \$	0	0	0,00 \$
Thaïlande	0	1	16 879,19 \$	0	0	0,00 \$	0	0	0,00 \$
Puerto Rico	0	1	2 839,00 \$	0	0	0,00 \$	0	0	0,00 \$
Inde	0	1	157,84 \$	0	0	0,00 \$	0	0	0,00 \$
Autriche	0	0	0,00 \$	0	1	5 530,55 \$	0	0	0,00 \$
Guatemala	0	0	0,00 \$	0	1	189,00 \$	0	0	0,00 \$
Pays-Bas	0	0	0,00 \$	0	0	0,00 \$	0	1	126,00 \$
Japon	0	0	0,00 \$	0	0	0,00 \$	0	1	162,50 \$

**Évaluation de la menace :
Fraude en marketing de masse**



**La perspective canadienne —
novembre 2007**

