La fraude par marketing de masse

Rapport au ministre de la Sécurité publique du Canada et à l'Attorney General des États-Unis

Mars 2008

***

Sous-groupe de la fraude par marketing de masse
Forum sur la criminalité transfrontalière

Tableau des matières

* * *

Introduction

En avril 1997, le Premier ministre du Canada, Jean Chrétien, et le Président des États-Unis, Bill Clinton, ont demandé que soit rédigée une étude conjointe des moyens de lutte contre la fraude transfrontalière par télémarketing qui se développait de façon inquiétante. En novembre 1997, un groupe de travail binational constitué à cet effet, a produit un rapport adressé au Premier ministre et au Président, lequel dresse un examen approfondi de la question et recommande plusieurs moyens d'améliorer la riposte des deux pays à ce difficile problème[1]. Le rapport recommandait notamment de reconnaître la gravité délictuelle du télémarketing frauduleux, de nommer des groupes de travail régionaux pour concrétiser la collaboration transfrontalière, d'harmoniser les stratégies de contrôle des activités de télémarketing frauduleux chevauchant la frontière, tant au niveau des divers services concernés qu'aux paliers régionaux et nationaux, de mettre sur pied un groupe de travail binational chargé de coordonner l'action et formuler diverses recommandations concernant la collecte de renseignements, la communication des preuves et des témoignages, l'entraide juridique, l'extradition, la sensibilisation du public et la prévention[2].

Le rapport de 1997 a servi de plan de coordination de la lutte binationale contre la fraude par télémarketing. Au cours des dix années qui se sont écoulées depuis la remise du rapport de 1997, le Canada et les États-Unis ont non seulement donné suite aux recommandations formulées, mais ont fait des progrès dans la lutte contre la fraude par marketing de masse, ces stratagèmes frauduleux au moyen de techniques de communications de masse telles que le télémarketing, l'Internet et la diffusion massive dans le but d'entrer en contact avec de grands nombres de victimes éventuelles pour essayer de leur soutirer de l'argent.

Le présent rapport répond à un triple objectif. Il s'agit dans un premier temps de décrire les évolutions constatées, depuis 2003, des quatre principaux types d'activités criminelles associées à la fraude par marketing de masse, soit les escroqueries par télémarketing, la fraude par Internet, les escroqueries liées au Nigeria[3] et le vol d'identité. Dans la seconde partie, nous résumerons les principales mesures prises par les services des deux pays depuis 2003 afin de lutter plus efficacement contre ce phénomène. Dans une troisième partie, nous évoquerons les recommandations que le sous-groupe avait formulées en 2003 dans le cadre du plan d'action binational de lutte contre la fraude par marketing de masse, avec une nouvelle recommandation liée à l'évolution des modes et des méthodes de fraude depuis 2003.

---

[1] Voir RAPPORT DU GROUPE DE TRAVAIL CANADA - ÉTATS-UNIS SUR LE TÉLÉMARKETING FRAUDULEUX, novembre 1997, ci-après Rapport de 1997, copie consultable à http://strategis.ic.gc.ca/pics/ctf/rapportf.pdf.

[2] Voir, p. ex., *id.*, aux pages 7, 20 à 22, 25, 28, 29.

[3] Certaines autorités canadiennes parlent de « Fraude liée à l'Afrique occidentale ».

Première partie : Le fraude par marketing de masse au Canada et aux États-Unis

Depuis plus de dix ans, le Canada et les États-Unis s'attachent à lutter contre la fraude par marketing de masse. Si à l'origine il s'agissait essentiellement de télémarketing frauduleux transfrontalier, la fraude par marketing de masse touchant les deux pays a, entre-temps, pris une telle extension qu'il constitue désormais un secteur d'activités criminelles multiformes comprenant non seulement le télémarketing frauduleux, connu depuis longtemps, mais la fraude par Internet, les escroqueries liées au Nigeria et le vol d'identité. Selon l'Évaluation de la menace liée au crime organisé Canada-États-Unis, 2006, le vol d'identité, la fraude par Internet et le blanchiment d'argent sont, en matière de criminalité financière, des activités qui gagnent actuellement en ampleur et en raffinement au niveau des moyens utilisés[4]. Ajoutons que l'évolution des moyens employés dans le cadre de stratagèmes de fraude par marketing de masse, notamment une très forte augmentation de l'emploi de faux chèques et de faux mandats, ainsi qu'un large recours aux divers mécanismes de paiement tels que les centres de traitement des paiements et les entreprises de transferts de fonds, compliquent sensiblement la lutte contre la fraude transfrontalière par marketing de masse.

Dans cette partie nous examinerons les principales tendances et évolutions constatées depuis 2003 en matière de fraude transfrontalière par télémarketing, de fraude par Internet, d'escroqueries liées au Nigeria et de vol d'identité.

A. La fraude par télémarketing

1. Contexte

La fraude par télémarketing est à la fois la forme de fraude la plus ancienne et, à certains égards, la plus persistante des escroqueries par marketing de masse contre lesquelles luttent le Canada et les États-Unis. Selon l'Évaluation de la menace liée au crime organisé Canada-États-Unis – 2006, les auteurs de fraudes par télémarketing continuent à s'en prendre aux citoyens des deux pays[5].

Aux États-Unis, selon les statistiques les plus récentes, la Ligue nationale des consommateurs (NCL), organisation américaine privée à but non lucratif, estime que les types les

[4] ÉVALUATION DE LA MENACE LIÉE AU CRIME ORGANISÉ CANADA - É.-U. - 2006, consultable à http://www.rcmp-grc.gc.ca/organizedcrime/octa_f.htm .

[5] *Id.*

plus répandus de fraude par télémarketing sont ceux qui correspondent aux données figurant au tableau I :[6]

TABLEAU I : NATIONAL CONSUMERS LEAGUE FRAUD CENTER DONNÉES RELATIVES À LA FRAUDE PAR TÉLÉMARKETING POUR L'ANNÉE 2006		
Type d'escroquerie	***Pourcentage de plaintes***	***Perte moyenne par victime***
1. Faux chèque	31	3 278 $
2. Jeux et concours truqués	26	2 749 $
3. Vente de magazines	8	77 $
4. Bourses d'études	6	236 $
5. Arnaque de prêts avec frais prépayés	6	1 164 $
6. Loteries / Clubs de loterie	6	3 189 $
7. Offres de carte de crédit	4	237 $
8. Hameçonnage	3	387 $
9. Projets d'emploi à domicile	1	104 $
10. Voyages / Vacances	1	812 $

Ces données appellent deux observations. D'abord, les fraudes au faux chèque, où l'on obtient de la victime qu'elle dépose à son compte en banque des chèques dont elle ne s'apercevra que plus tard qu'ils sont faux, et en contrepartie desquels est envoyée à l'escroc une partie seulement des chèques en questions, ont non seulement suscité le plus grand nombre de plaintes, mais sont en outre à l'origine des pertes moyennes les plus élevées. Ensuite, les pertes moyennes dues aux loteries et clubs de loterie frauduleux sont les deuxièmes en importance, mais ne sont à l'origine que de 6 p. 100 des plaintes, alors que les combines reposant sur des prix et concours fallacieux viennent, par leur fréquence, en deuxième position et sont parmi les fraudes par télémarketing responsables des pertes moyennes les troisièmes en importance.

Dans le cadre des données portant sur l'année 2006, la NCL a précisé qu'en ce qui concerne les combines de fraude par télémarketing visant les consommateurs américains, les cinq principaux lieux d'origine sont les suivants : 1) le Canada (30 %); 2) des pays autres que les États-Unis et le Canada (15 %; 3) la Floride (8 %; 4) New York (7 %) et 5) la Californie (5 %). Selon la NCL, 45 p. 100 des plaintes enregistrées en 2006 concernaient des stratagèmes de fraude par télémarketing

[6] *Voir* Ligue nationale des consommateurs, 2006 Top 10 Telemarketing Scam Trends from NCL's Fraud Center, janvier-décembre 2006, ci-après NCL 2006 TELEMARKETING TRENDS, consultable en anglais uniquement à http://fraud.org/stats/2006/telemarketing.pdf.

originant à l'étranger et visant de résidents des États-Unis, en augmentation de 26 p. 100 par rapport à 2006[7].

Au Canada, pour la période allant de 2005 à 2007, PhoneBusters, le Centre d'appel antifraude du Canada fait état des renseignements suivants sur les diverses offres frauduleuses :[8]

Tableau II : PhoneBusters, données relatives aux plaintes pour fraude reçues au cours de la période 2005-2007 (y compris les prix mensongers, les fausses offres de prêts ou de vacances, et divers autres types de combines)

	2005	***2006***	***2007***
Tentatives originant au Canada	11 306	10830	14433
Victimes canadiennes	4 608	4192	4124
Montant des pertes déclarées au Canada	16 498 990,70 $	24 532 680,04 $	18 177 921,36 $
Tentatives originant aux États-Unis	10 668	13 350	9 069
Victimes résidant aux États-Unis	12 214	10 908	8684
Montant des pertes déclarées aux États-Unis	58 432 710,73 $	48 830 098,19 $	35 438 164,96 $
Tentatives originant au Royaume-Uni	32	16	14
Victimes résidant au Royaume-Uni	115	47	56
Montant des pertes déclarées au Royaume-Uni	730 925,99 $	1 296 538,41 $	987 924,05 $
Tentatives originant dans d'autres pays ou de provenance inconnue	186	76	72
Victimes résidant dans divers autres pays ou dont le lieu de résidence, n'est pas connu	169	87	177

[7] Voir *id.*

[8] Voir Le centre d'appel antifraude du Canada, Phonebusters, Compte rendu succinct mensuel 2007, à http://www.phonebusters.com/francais/documents/Yearly2007Fr_001.pdf.

Tableau II : PhoneBusters, données relatives aux plaintes pour fraude reçues au cours de la période 2005-2007 (y compris les prix mensongers, les fausses offres de prêts ou de vacances, et divers autres types de combines)			
Montant des pertes déclarées dans d'autres pays	657 909,58 $	1 383 452,12 $	4 099 652,54 $
Nombre total de tentatives de fraude	22 192	24 272	23 588
Nombre total des victimes de fraudes	17 106	15 234	13 041
Montant des pertes déclarées à la suite d'une fraude	76 320 537,00 $	76 042 768,76 $	58 703 662,91 $

Ces données appellent plusieurs observations. D'abord, alors que le nombre de tentatives de fraude auprès de résidents canadiens a augmenté entre 2006 et 2007, le nombre actuel de résidents canadiens effectivement victimes est demeuré le même et le montant des pertes canadiennes a baissé d'un tiers. Deuxièmement, entre 2006 et 2007, le nombre de tentatives de fraude originant aux États-Unis et visant des résidents américains, ainsi que le nombre de victimes habitant les États-Unis et le montant total des pertes américaines (selon PhoneBusters) ont dans l'ensemble tous baissé. Troisièmement, le petit nombre de tentatives de fraude auprès de résidents du Royaume-Uni ainsi que le montant total des pertes enregistrées au Royaume-Uni ont légèrement baissé entre 2006 et 2007. Quatrièmement, le nombre de victimes résidant dans d'autres pays (ou dont le lieu de résidence n'est pas connu), ainsi que le montant total de leurs pertes, ont augmenté sensiblement entre 2006 et 2007, le nombre de victimes ayant plus que doublé, et le montant des pertes ayant presque triplé.

2. Les tendances constatées

Au cours des quelques dernières années, plusieurs éléments de la fraude transfrontalière par télémarketing n'ont guère changé. Il s'agit notamment du recours assez large aux entreprises de transfert de fonds pour toucher l'argent envoyé par les victimes. D'autres aspects de ce secteur d'activités criminelles ont cependant évolué sensiblement depuis 2003, comme nous allons le voir dans les pages qui suivent :

a. Le rôle du crime organisé

Le plus grand changement intervenu depuis 2003 au niveau de la fraude transfrontalière par télémarketing est le rôle croissant des bandes criminelles dirigées à partir du Nigeria dans la fraude par télémarketing et divers autres types de fraudes financières, y compris les stratagèmes de fraude

par Internet telles que le hameçonnage ou la pêche aux données personnelles[9] et diverses autres combines employant de faux chèques[10]. Selon les autorités, si tout porte à penser que certains éléments traditionnelles des organisations criminelles hiérarchisées continuent à jouer un rôle dans les fraudes transfrontalières par télémarketing, s'occupant en particulier de fournir des tuyaux, tels que les noms des personnes ayant déjà succombé à des fraudes, et divers renseignements les concernant) de la « protection »[11] des locaux où sont basées les opérations de fraude par télémarketing, le blanchiment d'argent, le nombre de combines frauduleuses originant au Nigeria a sensiblement augmenté dans plusieurs grandes villes du Canada, ainsi que dans plusieurs pays d'Afrique occidentale et certains pays européens tels que les Pays-Bas, l'Espagne et le Royaume-Uni. Ces associations de malfaiteurs liées à des nationaux nigérians emploient de nombreux complices dans le cadre de combines compliquées menées avec un grand souci du détail, les acolytes postés dans divers pays étant souvent chargés de fonctions très précises, même si on ne retrouve pas dans de telles bandes cette hiérarchisation caractéristique des diverses organisations criminelles à base ethnique opérant en Europe et en Amérique du Nord.

b. « Boniments » et autres artifices

En ce qui concerne les bandes criminelles autres que nigériane, au cours des cinq dernières années, on continue à voir employer, pour la fraude par télémarketing, bon nombre des « boniments » remontant à la première partie de la décennie, dont les diverses fables, sornettes et explications débitées par les criminels pour justifier les demandes d'argent qu'ils adressent à leurs futures victimes. Il peut s'agir de fausses offres de prix, ou de gains de concours ou de loterie, de fausses offres de prêt ou de carte de crédit garantis, de stratagèmes « interentreprises » (notamment d'offres d'inscription dans des bottins d'entreprises tout à fait fictifs, ou l'offre de produits ou des fournitures de bureau)[12]. Ces escroqueries peuvent rapporter beaucoup. Le copropriétaire de

---

[9] Voir p. 12, *infra*.

[10] Voir ÉVALUATION DE LA MENACE LIÉE AU CRIME ORGANISÉ CANADA - É.-U. - 2006, *supra*, note 4.

[11] D'autres organisations criminelles extorquent des escrocs le paiement d'un « impôt ».

[12] Au Canada, les stratagèmes interentreprises transfrontaliers semblent être concentrés dans la région de Montréal. Les autorités y ont déjà repéré environ 50 de ces stratagèmes de fraude interentreprise, qui, en général, emploient de 10 à 30 personnes. Mais, parfois, sensiblement plus. grandes. En octobre 2007, à Montréal, la police a effectué une descente dans les locaux servant à une escroquerie « interentreprises » occupant plusieurs étages d'un immeuble commercial et employant une centaine de « démarcheurs » (c.-à-d., d'employés chargés d'appeler les éventuelles victimes pour leur proposer une inscription dans un bottin d'entreprises ou des trousses de premiers soins. Il semblerait que cette escroquerie ait visé de petites et moyennes entreprises au Canada, aux États-Unis et en Europe. Plus de 120 personnes ont été arrêtées. Voir Jan Ravensbergen, *Alleged fraud ring busted*, *Montreal Gazette*, 9 octobre 2007, consultable en anglais uniquement à www.canada.com/globaltv/national/story.html?id=9b36522b-29f0-44ce-bcbd-c2a0ce2e147b

deux officines de télémarketing installées à Montréal et à Toronto et s'attaquant exclusivement à des entreprises américaines, leur proposant des inscriptions dans des bottins d'entreprises parfaitement fictifs et employant divers autres types de stratagèmes, a récemment été déclaré coupable de dix infractions à la *Loi sur la concurrence* en raison de représentations fausses ou trompeuses faites par le truchement de ses entreprises. Selon un calcul estimatif, les deux entreprises auraient eu un chiffre d'affaires de plus de 70 millions de dollars[13].

Suite à la multiplication, au Canada, de stratagèmes frauduleux originant au Nigeria, les autorités ont constaté l'emploi d'une gamme élargie de ces combines de frais d'emprunt payables à l'avance typiques des bandes criminelles nigérianes. Dans ce genre de stratagème, il peut s'agir d'offres frauduleuses où l'on tente d'obtenir de la victime éventuelle qu'elle verse à son compte bancaire un chèque envoyé par les malfaiteurs et qu'en contrepartie elle leur envoie, par virement télégraphique, une partie du montant inscrit sur le chèque. Il n'est pas rare que les victimes se laissent convaincre, s'apercevant trop tard qu'elles ont non seulement perdu l'argent envoyé aux escrocs, mais qu'elles doivent en plus rembourser intégralement le montant du chèque déposé à leur compte.

Selon les autorités, les auxiliaires de certaines combines montées par des bandes nigérianes contactent initialement la victime par courrier, mais se servent ensuite du téléphone pour entretenir le contact avec les personnes ayant répondu favorablement au courrier initial. Rappelons que certains stratagèmes émanant de pays d'Afrique occidentale visent le vol d'identité, employant l'Internet pour extirper des données personnelles et financières concernant les victimes.

c. Techniques de dissimulation

Selon les autorités, les stratagèmes de fraude transfrontalière ont de plus en plus recours à la Voix sur réseau IP (VoIP).

> On entend par VoIP, une technologie permettant de placer les appels en utilisant non pas les lignes téléphoniques ordinaires (avec transmission analogique des données) mais une connexion Internet à large bande. Certains services VoIP ne permettent de contacter que les personnes abonnées au même service, mais certains autres permettent de contacter toute personne ayant un numéro de téléphone, que ce numéro soit local, interurbain, portable ou branché dans un autre pays. Ajoutons que certains

---

ou voir *Le COLT cible une organisation soupçonnée d'être impliquée dans le fraude par marketing de masse* disponible seulement en français à
http://www.rcmp-grc.gc.ca/qc/comm/archives/2007/10/071009_f.htm

[13] Voir Paul Cherry, *Bogus telemarketing head guilty of violating competition laws, Montreal Gazette*, 26 février, 2008, consultable en anglais uniquement à
http://www.canada.com/montrealgazette/news/story.html?id=bd5d6d66-9ece-49a1-a09d-e629ca7584eb&k=76148.

services VoIP exigent l'utilisation d'un ordinateur ou d'un téléphone VoIP spécial, mais que d'autres services permettent d'employer un téléphone ordinaire dans la mesure où il est raccordé à un adaptateur VoIP[14].

Les services VoIP permettant à l'utilisateur d'afficher à l'intention du destinataire de l'appel un numéro de téléphone qui ne correspond pas au lieu où se trouve celui qui appelle. Cela permet de tromper l'éventuelle victime en lui faisant croire que l'appel provient d'ailleurs. Ainsi, des escrocs installés en Floride peuvent faire afficher sur le téléphone de la victime l'indicatif régional 212 (New York), ou des escrocs au prêt avec frais payables à l'avance, installés à Toronto, peuvent faire en sorte que soit affiché à l'autre bout de la ligne un code régional n'ayant rien à voir avec Toronto. Selon les autorités, la technologie VoIP est employée, à partir du Canada et du Costa Rica, dans le cadre de grandes opérations de fraude par télémarketing visant des résidents des États-Unis.

d. Transferts monétaires

On peut dire, de manière générale, qu'entre 2003 et 2008, les victimes ont continué à se laisser convaincre d'envoyer leur argent par virement télégraphique, notamment par l'intermédiaire des deux principales entreprises spécialisées, Western Union et MoneyGram. Aux États-Unis, selon la Ligue nationale des consommateurs, en 2006, le virement télégraphique était de loin le principal mode de paiement employé dans les stratagèmes de télémarketing. En effet, 54 p. 100 des plaintes enregistrées faisaient état de ce mode de paiement. Dans 35 p. 100 des plaintes, trois autres formes de paiement avaient été employées : 2) le débit bancaire, (14 %); 3) le paiement par chèque, (11 %); et le paiement par carte de crédit, (10 %)[15].

Les autorités ont découvert, au début de la présente décennie, que des membres d'organisations criminelles ont parfois, et notamment au Québec, essayé soit de compromettre, soit de menacer des employés des services de transfert de fonds afin de les persuader de ne pas remplir les formalités requises pour les sommes transférées par les victimes de machinations frauduleuses. Dans certaines régions du Canada, afin de mieux dissimuler leurs agissements, des membres d'organisations criminelles nigérianes ont obtenu des franchises Money Gram et Western Union. Ces franchises ne sont que des paravents employés, non dans le cadre d'une entreprise légitime, mais uniquement pour blanchir le produit d'activités illicites.

---

[14] Federal Communications Commission, IP-Enabled Services, consultable en anglais uniquement à http://www.fcc.gov/voip/.

[15] Voir NCL 2006 TELEMARKETING TRENDS, supra, note 6.

B. La fraude par Internet

1. Le contexte

Depuis la création du Web, les autorités policières d'Amérique du Nord ont pu constater la grande diversité des stratagèmes frauduleux ayant recours à l'Internet tant pour établir le contact initial avec la victime éventuelle que pour recevoir le paiement et blanchir les sommes recueillies. Le rapport publié en février 2008 par la Federal Trade Commission (FTC) contient les statistiques les plus récentes sur les plaintes enregistrées aux États-Unis en matière de fraude par Internet. Ces données regroupées au tableau III, rendent compte des plaintes enregistrées par la FTC au cours de la période 2005 à 2007[16] :

Tableau III : Plaintes enregistrées par la FTC entre 2005-2007 en matière de fraude par Internet			
	2005	***2006***	***2007***
Nombre de plaintes	197 085	205 269	221 226
Montant total des pertes déclarées	336 345 604 $	590 494 777 $	525 743 643 $
Perte moyenne	2 095 $	3 332 $	2 730 $
Perte médiane[17]	342 $	500 $	395 $

Ces données appellent plusieurs observations. Le nombre de plaintes enregistrées en 2007 pour fraude par Internet a augmenté de presque 8 p. 100 par rapport à 2006, mais le total des pertes, le montant moyen des pertes ainsi que la médiane de ces pertes enregistrent une baisse par rapport à l'année précédente. Cela dit, le total des pertes déclarées en 2007 dépasse tout de même 525 millions de dollars, montant exceptionnellement élevé par rapport aux autres types de fraude. Les sommes versées, en moyenne, par les victimes de fraude par Internet (c.-à-d., le montant total des pertes divisé par le nombre de victimes ayant déclaré le montant du versement effectué) sont, au cours des trois années en question, sensiblement supérieures à la médiane et il semble donc qu'un certain nombre de versements particulièrement importants aient eu pour effet de biaiser, pour chacune des trois années en cause, la moyenne des versements effectués. Ainsi, en 2007, selon les données relatives aux plaintes enregistrées, 83 p. 100 de ces plaintes faisaient état d'une perte de 1 000 $ ou

---

[16] Voir FEDERAL TRADE COMMISSION, CONSUMER FRAUD AND IDENTITY THEFT COMPLAINT DATA: JANUARY-DECEMBER 2007, février 2008, ci-après cité sous la forme FTC 2007 COMPLAINT DATA, consultable en anglais uniquement à http://www.ftc.gov/opa/2008/02/fraud.pdf.

[17] Selon la FTC cette « médiane correspond à la valeur qui partage le total en deux sous-ensembles, la moitié des chiffre d'un premier groupe ayant une valeur supérieure à la médiane, les chiffres du deuxième groupe ayant une valeur inférieure. Le calcul de la médiane ne tient pas compte des plaintes portant sur des tentatives de fraude si la victime n'a effectué aucun versement. *Id.*, p. 10.

moins, 12 p. 100, (soit 22 458 au total) concernant des versements allant de 1 000 à 5 000 $, 4 p. 100 des plaintes (ou 7 017) faisant état d'un versement de plus de 5 000 $[18].

2. Tendances constatées

Voici, regroupées au tableau IV, les données recueillies aux États-Unis par la FTC et retraçant l'évolution des modes de paiement entre 2005 et 2007[19] :

Tableau IV : Modes de paiement signalés à la FTC par des consommateurs portant plainte pour fraude par Internet – 2005-2007 [montant des paiements (nombre de plaintes)]

	2005	***2006***	***2007***
Compte bancaire débité	11 181 001 $ (6 153)	21 792 498 $ (6 643)	13 751 585 $ (6 653)
Espèces / Avance en espèces	11 164 636 $ (1 039)	7 648 293 $ (1 169)	7 943 260 $ (1 216)
Chèques	21 804 907 $ (3 437)	60 119 725 $ (2 850)	17 906 180 $ (2 577)
Cartes de crédit	19 004 962 $ (12 208)	24 736 839 $ (12 927)	30 681 611 $ (14 822)
Mandat	7 839 943 $ (3 997)	16 661 396 $ (3 660)	25 663 620 $ (2 962)
Note de téléphone	96 364 $ (424)	259 659 $ (429)	112 452 $ (298)
Virement télégraphique	41 786 350 $ (5 557)	91 623 738 $ (8 769)	76 670 821 $ (10 857)

Ces données sont intéressantes à plusieurs égards. D'abord, les versements par virement télégraphique demeurent, par l'importance des sommes en cause, le principal mode de paiement, même si le total des montants envoyés par virement télégraphique en 2007 a baissé par rapport à 2006 alors que, au cours de cette période, le nombre de plaintes signalant ce mode de versement a augmenté de presque 24 p. 100. Deuxièmement, comme mode de paiement, les cartes de crédit restent loin derrière les virements télégraphiques alors même que le montant des versements effectués par carte de crédit a augmenté de 24 p. 100 par rapport à 2006. Ajoutons que le versement moyen effectué en 2007 par carte de crédit (2 070 $) a augmenté de plus de 8 p. 100 par rapport à 2006. Troisièmement, entre 2006 et 2007, on constate une baisse sensible à la fois du total des sommes versées par chèque (ce total passant de 60 millions de dollars à environ 18 millions de dollars) et des sommes débitées d'un compte bancaire (passant de presque 22 millions de dollars à 14 millions de dollars), même si le nombre de plaintes faisant état de ce mode de versement n'a pas sensiblement

[18] *Id.*

[19] Voir *id.*, à la page 11.

changé d'une année à l'autre. Quatrièmement, on relève, entre 2006 et 2007, une augmentation sensible des paiements effectués par mandat (le total passant de plus de 16 millions de dollars à plus de 25 millions de dollars), bien que le nombre de plaintes faisant état de mode de paiement ait baissé de presque 24 p. 100 au cours de cette période.

D'autres données se rapportant aux tendances constatées en ce domaine ont été réunies par le Internet Crime Complaint Center (IC3), partenariat entre le FBI et le National White Collar Crime Center. Au vu des plaintes enregistrées en 2006, le IC3 fait état des résultats suivants :

> Pour l'ensemble des fraudes déclarées, les pertes se sont élevées, au total, à 198,44 millions de dollars, la médiane étant de 724 $ par perte enregistrée. Cela constitue donc une augmentation par rapport aux pertes de 183,12 millions de dollars enregistrées en 2005. L'analyse des plaintes déposées a en outre permis de constater que :
>
> - l'infraction la plus fréquente, totalisant 44,9 p. 100 des plaintes déposées, a été la fraude en matière de vente aux enchères sur l'Internet. Dix-neuf pour cent des plaintes visaient des marchandises jamais livrées ou des versements non effectués. 4,9 p. 100 des plaintes visaient des fraudes par chèque. Les sept autres grandes catégories de plaintes déposées au cours de cette année étaient la fraude par carte de crédit / carte de débit, la fraude informatique, l'escroquerie et la fraude prétextant la participation d'un établissement financier.
>
> - Parmi les personnes ayant fait état d'une perte financière, la perte médiane la plus élevée était liée à la fraude nigériane par lettre (5 100 $), la fraude par chèque (3 744 $), et la fraude aux investissements (2 695 $).
>
> - Parmi les auteurs de ces fraudes, on relève 75,2 p. 100 d'hommes, dont la moitié domiciliés dans l'un des États suivants : la Californie, New York, la Floride, le Texas, l'Illinois, la Pennsylvanie et le Tennessee. La majorité de ces escrocs étaient basés aux États-Unis, mais un nombre appréciable d'entre eux opérait à partir du Royaume-Uni, du Nigeria, du Canada, de la Roumanie et de l'Italie.
>
> - On relève, parmi les personnes ayant porté plainte, 61,2 p. 100 d'hommes, dont la moitié âgés de 30 à 50 ans, un tiers d'entre eux habitant l'un des quatre États les plus peuplés des États-Unis, la Californie, le Texas, la Floride et New York. La plupart des personnes portant plainte résidaient aux États-Unis, mais le IC3 a également reçu un certain nombre de plaintes du Canada, de Grande-Bretagne, d'Australie, d'Inde et d'Allemagne.

- Le IC3 a récemment relevé de nombreux incidents de la ruse du tueur à gages, des tentatives de hameçonnage au moyen de sites truqués et d'escroqueries au moyen de faux chèques[20].

Selon la Ligue nationale des consommateurs (NCL), les dix principaux stratagèmes de fraude par Internet constatés en 2006 correspondent aux données du tableau V[21]. Plusieurs détails méritent d'être relevés. D'abord, les stratagèmes de fraude aux investissements en ligne semblent avoir fortement augmenté en 2006. Des dix principaux types de fraude par Internet relevés en 2006, ce type de fraude a entraîné les pertes moyennes les plus élevées, mais c'est la première fois en dix ans que ce type d'escroquerie se place parmi les dix premières sortes de fraude[22]. Deuxièmement, les escroqueries par faux chèque arrivent en deuxième position pour la moyenne des pertes, même si elles ne comptent que pour 11 p. 100 des plaintes déposées auprès de la NCL. Bon nombre de ces fraudes par faux chèque étant le fait d'organisations criminelles provenant d'Afrique occidentale, il est possible que certaines des bandes qui en sont responsables soient également à l'origine d'autres stratagèmes ayant fait l'objet de plaintes, et notamment les fraudes nigérianes qui consistent à offrir, au départ, de l'argent à la victime éventuelle.

Tableau V : Plaintes déposées en 2006 auprès de la NCL (É.-U.) pour fraude par Internet

	Pourcentage de l'ensemble des plaintes	*Perte moyenne*
1. Ventes aux enchères	34	1 331 $
2. Marchandises diverses	33	1 197 $
3. Escroqueries au faux chèque	11	4 053 $
4. Promesses financières du Nigeria	7	3 741 $
5. Loteries / Clubs de loterie	4	1 750 $
6. Prêts avec frais prépayés	3	1 515 $
7. Hameçonnage	2	Aucune perte signalée
8. Prix / Concours	1	2 447 $
9. Services d'accès à l'Internet	1	$920

[20] INTERNET CRIME COMPLAINT CENTER, INTERNET CRIME REPORT : JANUARY 1, 2006 - DECEMBER 31, 2006 à la p. 3, 2007, consultable en anglais uniquement à http://www.ic3.gov/media/annualreport/2006_IC3Report.pdf.

[21] Voir National Consumers League, 2006 Top 10 Internet Scam Trends from NCL's Fraud Center, January – December 2006, consultable en anglais uniquement à http://fraud.org/stats/2006/internet.pdf.

[22] *Id.*

Tableau V : Plaintes déposées en 2006 auprès de la NCL (É.-U.) pour fraude par Internet		
10. Investissements	1	$4,759

Troisièmement, comme pour les plaintes déposées auprès de la NCL pour fraude par télémarketing, pour ce qui est des plaintes pour fraude par Internet, les virements télégraphiques sont, de loin, le principal mode de paiement (45 %). Citons, parmi les autres modes de paiement utilisés dans ce genre de fraudes, les cartes de crédit (20 %); les débits bancaires (9 %); la carte de débit (8 %); les mandats (8 %); les chèques (5 %); les chèques de banque (2 %); et les espèces (2 %)[23]. Et enfin, les cinq principaux lieux d'origine des fraudes par Internet déclarées à la NCL étaient 1) des pays autres que les États-Unis et le Canada (38 %); 2) la Californie (10 %); 3) la Floride et New York (6 %, ex æquo); 5) le Texas et le Canada (4 %, ex æquo); et 7) l'Illinois (3 %)[24].

C. Escroqueries liées au Nigeria

Le troisième type important de fraude par marketing de masse dont il soit fait état dans le rapport 2003 est la fraude originant au Nigeria, c.-à-d., les stratagèmes mis sur pied par des organisations criminelles à structure élastique entretenant des liens avec le Nigeria. Il s'agit de divers types d'offres frauduleuses effectuées par courrier, par télécopie, par téléphone ou par courriel. La victime éventuelle peut ainsi se voir offrir des occasions bidons d'aider des résidents africains à blanchir des bénéfices illicites ou à transférer certaines sommes hors d'Afrique. Les spécialistes nord-américains, européens et nigérians de ce genre de fraudes, s'accordent pour dire que quel que soit le type précis de stratagèmes employé ou le principal lieu d'opération, ce genre d'escroquerie est le fait de réseaux criminels à structure souple sur lesquels règnent des individus de nationalité nigériane ou entretenant avec le Nigeria des liens tribaux ou familiaux, même si le personnel subalterne peut comprendre des gens provenant d'autres pays d'Afrique occidentale ainsi que des non-Africains.

Même si on ne possède pas pour les États-Unis de données globales concernant le nombre de résidents des États-Unis contactés dans le cadre de ce genre de combines, le Consumer Fraud and Identity Theft Complaint Data de 2008 du FTC indique que "Des offres de fonds étrangers" est le quatrième en grandeur des catégories des plaintes dans la base de donnés de Consumer Sentinel (ou 4% du total). Au Canada, PhoneBusters a réuni des données concernant les stratagèmes nigérians par envoie de lettres. Le tableau VI rend compte des données concernant la période 2005 à 2007[25] :

[23] Voir *id.*

[24] Voir *id.*

[25] Voir Le centre d'appel antifraude du Canada, Phonebusters, Compte rendu succinct mensuel 2007, *supra*, note 8.

Tableau VI : Récapitulation des plaintes déposées, entre 2005 et 2007, auprès de PhoneBusters pour escroqueries par lettre de type nigérian			
	2005	***2006***	***2007***
Victimes canadiennes	175	192	152
Total des pertes déclarées	9 168 422,34 $	3 056 355,18 $	5 264 488,15 $

Ces données appellent quelques observations. En 2007, la perte moyenne atteint presque 35 000 $. Cela représente une forte augmentation par rapport à la perte moyenne de 16 000 $ enregistrée en 2006, même si, en 2007, le nombre de victimes canadiennes portant plainte est sensiblement inférieur aux chiffres de 2006. Il est tout à fait possible qu'une ou deux des victimes aient déclaré des pertes pouvant atteindre plusieurs centaines de milliers de dollars, voire plus d'un million de dollars et qu'un ou deux cas aient sensiblement biaisé à la hausse le montant moyen des pertes pour l'année. Cela dit, les autorités policières ont constaté qu'au départ certaines victimes de ces escroqueries nigérianes minimisent le montant de leurs pertes, en partie parce qu'elles ont du mal à en admettre l'importance, bien qu'elles aient décidé de porter plainte.

À moins de procéder à des enquêtes approfondies, il est particulièrement difficile de calculer les pertes découlant de telle ou telle escroquerie en provenance d'Afrique. Les autorités policières des deux pays considèrent néanmoins que ces stratagèmes frauduleux partis du Nigeria constituent, tant au Canada qu'aux États-Unis, une menace grandissante pour les consommateurs.

D. Le vol d'identité

1. Contexte

Au cours des cinq dernières années, le vol d'identité s'est répandu dans toutes les régions d'Amérique du Nord. Cette forme de criminalité touche tous les secteurs de la société, y compris les entreprises et les établissements financiers. Les autorités policières font généralement une distinction entre le vol d'identité et la fraude par marketing de masse. Certains stratagèmes de vol d'identité sont le fait de criminels qui tentent, par des arguments trompeurs et frauduleux, d'obtenir que leurs victimes leur révèlent des données personnelles et financières.

Au Canada, en matière de vol d'identité, PhoneBusters a réuni, pour la période de 2005 à 2007, les renseignements figurant au tableau VII[26] :

Tableau VII : Plaintes déposées entre 2005 et 2007 auprès de PhoneBusters pour vol d'identité			
	2005	***2006***	***2007***

[26] Voir *id.*

Tableau VII : Plaintes déposées entre 2005 et 2007 auprès de PhoneBusters pour vol d'identité			
Canadiens à risque	731	730	311
Victimes canadiennes	12859	13221	4633
Montant déclaré des pertes	8 683 603,54 $	15 734 254,69 $	6 383 477,37 $

Les plaintes déposées auprès de PhoneBusters pour vol d'identité montrent qu'entre 2006 et 2007, le nombre de victimes canadiennes ainsi que le montant de leurs pertes ont très sensiblement diminué.

Aux États-Unis, selon la FTC, en 2007, et dans les années précédentes, le vol d'identité a été, en matière de fraude contre le consommateur, à l'origine du plus grand nombre de plaintes. En 2005, le vol d'identité est à l'origine de 255 627 plaintes, de 246 124 plaintes en 2006 et de 258 427 en 2007[27].

2. Tendances et évolutions en matière de vol d'identité

Les organismes policiers des deux pays ne disposent pas encore de données statistiques globales leur permettant de cerner de manière précise les tendances en matière de vol d'identité. Les données statistiques et autres qu'elles ont pu réunir au cours des cinq dernières années, leur a permis néanmoins, de se faire une meilleure idée des principales tendances qui se dégagent.

a. Techniques employés en matière de vol d'identité

1) *L'hameçonnage*

Parmi les techniques utilisées pour le vol d'identité, il y en a une, l'hameçonnage, ou pêche aux données personnelles, sur laquelle on possède des données statistiques portant sur une période relativement longue. De manière générale, on entend par hameçonnage, la création et l'utilisation à des fins criminelles de courriels et de sites Internet mimant les sites d'entreprises et d'établissements financiers légitimes afin d'obtenir, par ces faux-semblants, que les victimes divulguent des données personnelles et financières qui peuvent être employées à leur détriment. Selon l'Évaluation de la menace liée au crime organisé Canada-États-Unis – 2006, les stratagèmes de pêche aux données personnelles est, pour les usagers de l'Internet, ce qui présente le plus grand risque au niveau du vol d'identité. C'est également, dans ce domaine, un des modes d'escroquerie les plus rentables[28].

---

[27] Voir FEDERAL TRADE COMMISSION, CONSUMER FRAUD AND IDENTITY THEFT COMPLAINT DATA: JANUARY - DECEMBER 2007, à la page 4, février 2008.

[28] ÉVALUATION DE LA MENACE LIÉE AU CRIME ORGANISÉ CANADA - É.-U. - 2006, *supra*, note 4.

Selon les données statistiques recueillies par le Anti-Phishing Working Group (APWG), association sectorielle s'attachant à éliminer le vol d'identité et la fraude d'identité par la pêche de données personnelles et par l'usurpation de courriels, on constate, depuis 2003, en matière d'hameçonnage, quatre tendances distinctes :

- **Incidence et prévalence de la pêche aux données personnelles ou hameçonnage**. Ce phénomène peut-être, des diverses formes de vol d'identité touchant l'Amérique du Nord, celle qui a le plus radicalement augmenté au cours des cinq dernières années. En janvier 2004, l'APWG a publié son premier rapport sur l'émergence de ce nouveau problème. Selon l'APWG, au cours du mois en question, il a été fait état de 176 opérations d'hameçonnage. À l'époque, ce nombre de tentatives a été jugé significatif, étant donné qu'il représentait une augmentation de 52 p. 100 par rapport au nombre d'attaques signalées en décembre 2003[29].

  Depuis lors, l'incidence et la prévalence de la pêche aux données personnelles ont crû au-delà des prévisions les plus pessimistes des spécialistes tant du secteur public que du secteur privé. En novembre 2007, 28 074 incidents d'hameçonnage ont été signalés à l'APWG, cet organisme ayant en outre répertorié 23 630 sites d'hameçonnage hébergés dans diverses régions du monde[30]. Les sites Internet employés pour la pêche aux données personnelles sont en effet installés dans de nombreux pays, y compris les États-Unis et divers pays d'Asie et d'Europe. Selon l'APWG, en novembre 2007, les dix principaux pays abritant des sites de pêche aux données personnelles étaient : 1) la Chine (24,21 %); 2) les États-Unis (23,85 %); 3) l'Inde (9,39 %); 4) la Fédération de Russie (8,06 %); 5) la Thaïlande (4,64 %); 6) la Roumanie (3,53 %); 7) l'Allemagne (3,41 %); 8) la République de Corée (2,42 %); 9) le Royaume-Uni (1,47 %); et 10) la France (1,47 %)[31].

- **Ciblage de divers secteurs industriels.** La pêche aux données personnelles a toujours privilégié l'industrie des services financiers mais celle-ci est depuis devenue la cible presque exclusive de ce genre d'activités. Selon l'APWG, en janvier 2004, 40 p. 100 des cas d'hameçonnage impliquaient le détournement d'appellations commerciales d'entreprises du secteur financier même si, au départ, certaines grosses entreprises de commerce électronique, telles que eBay, avaient, elles aussi, fait l'objet d'un nombre relativement important

---

[29] Voir ANTI-PHISHING WORKING GROUP, PHISHING ATTACK TRENDS REPORT: JANUARY, 2004, aux pages 1 et 3, 2004, cité sous la forme APWG, JANVIER 2004 TRENDS REPORT], consultable en anglais uniquement à http://www.antiphishing.org/reports/APWG.Phishing.Attack.Report.Jan2004.pdf.

[30] Voir ANTI-PHISHING WORKING GROUP, PHISHING ACTIVITY TRENDS: REPORT FOR THE MONTH OF NOVEMBER, à la page 1, 2008, ci-après APWG NOVEMBER 2007 TRENDS REPORT], consultable en anglais uniquement à http ://www.antiphishing.org/reports/apwg_report_nov_2007.pdf.

[31] *Voir id*., à la page 6.

d'offensives de ce genre[32]. Par contre, selon l'APWG, pour le seul mois de novembre 2004, 178 appellations commerciales ont été détournées dans le cadre d'opérations d'hameçonnage. Jamais un aussi grand nombre d'appellations commerciales n'avaient été détournées en un mois. Ce mois-là, 93,8 p. 100 de tous les cas d'hameçonnage visaient des entreprises appartenant au secteur des services financiers[33]. En novembre 2007, toujours selon l'APWG, outre un grand nombre d'établissements bancaires et de coopératives de crédit américains, un nombre croissant d'entreprises de services financiers de pays du Moyen-Orient et d'Europe ont été la cible de ce genre d'offensives[34].

- **Ciblage de certains individus en particulier.** Au cours des cinq dernières années, les spécialistes de la police et de la sécurité informatique ont constaté une augmentation des cas de pêche aux données personnelles visant des groupes précis d'individus. Cette technique d'hameçonnage, parfois appelée « harponnage » permet d'accroître le pourcentage d'individus aux données personnelles desquelles certains intérêts criminels peuvent obtenir accès.

  L'APWG a récemment fait savoir que le nombre de cas d'hameçonnage déclarés en novembre 2007, marquait une baisse de plus de 10 600 cas par rapport au mois précédent. Selon les analystes spécialisés, cette baisse serait en partie due au fait que les organisations criminelles tentent maintenant davantage de « harponner », les dirigeants de certaines entreprises afin de se procurer des renseignements leur permettant de s'en prendre après cela aux avoirs de l'entreprise[35]. Ces analystes ont notamment appris que des dirigeants d'entreprise se voient actuellement envoyer des courriels spécialement ciblés avec un double objectif : 1) installer sur leur ordinateur un maliciel [c.-à-d., un logiciel pernicieux] permettant aux harponneurs de pénétrer les systèmes de l'entreprise; et 2) d'obtenir accès aux comptes bancaires de l'entreprise[36].

- **L'installation de maliciels.** En janvier 2004, l'APWG a fait savoir que, dans la majorité des cas, l'hameçonnage est amorcé par un lien à un site Internet, bien que, dans quelques cas, il soit demandé aux destinataires de télécharger un fichier (contenant, en général, un virus ou programme de type cheval de Troie [c.-à-d., un programme qui semble assurer une fonction anodine mais qui, en fait, comporte un code malveillant])[37]. L'APWG ajoute que,

---

[32] *Voir* APWG JANUARY 2004 TRENDS REPORT, *supra*, note 29, à la page 1.

[33] *Voir* APWG NOVEMBER 2007 TRENDS REPORT, *supra*, note 30, aux pages 1 et 5.

[34] *Voir id.*, à la page 5.

[35] *Id.*, à la page 3.

[36] *Id.*

[37] *Voir* APWG JANUARY 2004 TRENDS REPORT, *supra*, note 26, à la page 3.

> Dans un petit nombre de cas, (cinq en l'occurrence), le message qu'il est demandé aux destinataires de télécharger et d'afficher comprend une annexe troyenne. Ces annexes contiennent en général des programmes permettant d'épier subrepticement les touches employées par la victime éventuelle (keylogging) et de repérer les frappes qui semblent correspondre à des numéros de cartes de crédit ou à des numéros d'assurance sociale, ou de calquer les fenêtres d'affichage comprenant le nom d'une banque ou d'une compagnie de carte de crédit. Le programme enregistre sur un fichier texte les données introduites au moyen du clavier, puis, par un système de courriel intégré, transmet les données à une boîte aux lettres électronique d'où elles peuvent être récupérées[38].

Selon l'APWG, les chevaux de Troie et les programmes de keylogging étaient, en novembre 2007, devenus les principales armes d'hameçonnage. Au cours du mois en question, l'APWG a relevé l'emploi de 3 500 localisateurs uniformes de ressources (adresses URL)[39] contenant des maliciels permettant de découvrir le mot de passe des personnes se servant de l'ordinateur[40]. Encore selon l'APWG, les dix principaux pays abritant des sites Internet hébergeant des enregistreurs de frappe ou des téléchargeurs troyens téléchargeant des keyloggers en aval étaient : 1) les États-Unis (68,93 %); 2) la Fédération de Russie(13,88 %); 3) la Chine (7,88 %); 4) la République de Corée (1,77 %); 5) le Royaume-Uni (1,67 %); 6) la Pologne (1,53 %); 7) l'Allemagne (1,38 %); 8) la France (1,13 %); 9) le Maroc (0,94 %); et 10) la Roumanie (0,89 %)[41].

En novembre 2007 également, l'APWG a en outre relevé l'utilisation de 338 maliciels permettant de s'emparer de mots de passe, soit une légère baisse par rapport au nombre relevé en 2007 (359). Cela représente néanmoins le plus grand nombre d'applications de ce genre constatées en un seul mois depuis janvier 2007 (345)[42].

---

[38] *Id.*, à la page 4.

[39] On entend par URL l'adresse universelle d'un site Web, d'un document ou d'une autre ressource se trouvant sur Internet. Une telle adresse universelle comprend deux parties : 1) un identificateur de protocole (http ou ftp) indiquant le protocole Internet donnant accès à cette adresse; et 2) un nom de ressource précisant l'adresse du protocole Internet (IP) ou le nom de domaine où se trouve cette ressource. Voir Webopedia, http://www.webopedia.com.

[40] Voir APWG NOVEMBER 2007 TRENDS REPORT , *supra*, note 27, à la page 7.

[41] Voir *id.*, à la page 8.

[42] *Id.*, à la page 7.

> L'APWG fait également état d'une forte augmentation du nombre de « redirecteurs de trafic » (c.-à-d., de maliciels permettant de réorienter les communications d'un usager d'Internet vers une destination non conforme aux intentions de l'utilisateur). Selon l'APWG, le plus grand nombre de ces redirecteurs de trafic Internet se trouvent dans un maliciel modifiant les paramètres du serveur du système de nommage de domaine Internet de l'utilisateur (système DNS) ou réorientant vers un service DNS frauduleux soit certaines soit toutes consultations DNS. Pour la plupart des domaines, le serveur frauduleux donne de bonnes réponses, mais il modifie sa réponse afin d'orienter l'utilisateur vers certains sites frauduleux (notamment vers des sites Internet d'hameçonnage mimant le site des établissements financiers dont l'utilisateur est client). Ainsi que l'explique l'APWG, ce type de stratagème est particulièrement efficace car l'assaillant peut, à tout moment, réorienter la recherche de l'utilisateur, et l'utilisateur final n'a que très peu de chances de s'apercevoir de ce qui se passe étant donné qu'il est en train de taper l'adresse sans se préoccuper du courriel ou du message SMS qui sert de leurre[43].

Tant au Canada qu'aux États-Unis, chacune de ces tendances est une forte source de préoccupations pour les entreprises et organismes d'application de la loi. Le recours croissant à des maliciels et à l'infection de sites Internet, est particulièrement préoccupant. Confirmant les constatations de l'APWG, une des principales entreprises de sécurité informatique a récemment indiqué qu'elle repère chaque jour 6 000 nouvelles pages Web infectées. Selon elle, moins de 20 p. 100 de ces pages Web sont le fait de pirates informatiques (c.-à-d., de sites malveillants). En effet, 83 p. 100 étaient des sites parfaitement légitimes qui avaient été compromis[44].

En réponse à cette augmentation radicale du nombre de cas d'hameçonnage, les sites Internet de nombreux établissements financiers du Canada et des États-Unis affichent dorénavant une mise en garde avertissant les clients des risques d'hameçonnage et leur expliquant comment signaler de tels incidents[45]. Les autorités publient, elles aussi, de plus en plus d'avertissements au sujet de la pêche aux données personnelles, soit sur leur site Internet, soit dans le cadre de rapports électroniques spéciaux à l'intention du public[46]. Ajoutons, que les établissements financiers et les organismes

---

[43] *Id.*, à la page 8.

[44] Voir SOPHOS, SECURITY THREAT REPORT, à la page 2, 2008, disponible en anglais seulement http://www.sophos.com/security/whitepapers/sophos-security-report-2008.

[45] Voir, par exemple, Fraude par courriel (hameçonnage), consultable à www.cibc.com/ca/legal/phishing-info-fr.html, MBNA Canada, Fraude - signalement et prévention, consultable à http://www.mbna.ca/fraud_protect.html; RBC, Fraude par courriel et faux site Web (pêche aux données personnelles), consultable à http://www.rbc.com/securite/bulletinPhishingf.html.

[46] Voir, par exemple, BINATIONAL WORKING GROUP ON CROSS-BORDER MASS-MARKETING FRAUD, SPECIAL REPORT ON PHISHING, octobre 2006, consultable à http://www.usdoj.gov/opa/report_on_phishing.pdf;

d'application de la loi, adressent également au public des mises en garde particulières à chaque fois qu'elles décèlent la présence de ce genre de manoeuvres[47].

2) Autres techniques de vol d'identité

Les autorités policières des deux pays ont constaté que les malfaiteurs ont recours à tout un éventail de techniques de vol d'identité, du hameçonnage à l'aide de techniques employées, jusqu'à des méthodes d'une faible technicité. Voici certaines des principales techniques constatées dans les deux pays[48] :

- **La fouille de poubelles**. Citons, parmi les techniques les plus simples de vol d'identité, la fouille de poubelles, procédé qui continue à être employé ici et là. Il s'agit de récupérer dans les poubelles et les bennes à ordures des documents mis aux rebuts par les entreprises, des quittances ou des relevés bancaires, par exemple.

- **Le vol ou la compromission de données par des employés ou des initiés.** Les employés d'entreprises, d'établissements financiers ou d'organismes gouvernementaux peuvent décider de voler sur leurs lieux de travail, ou de divulguer des données personnelles de nature délicate, soit pour en faire eux-mêmes usage soit pour les vendre ou les divulguer à d'autres.

- **Le « piquage » de NIP.** Il arrive que dans des lieux publics, tels que les aéroports, les guichets automatiques et les hôtels, des malfaiteurs se postent près des téléphones publics ou des guichets automatiques afin de voir s'ils peuvent entendre ou épier de précieux renseignements tels qu'un numéro de carte de crédit ou le NIP ouvrant accès à un guichet automatique.

- **L'« écrémage ».** Il s'agit d'une variante plus recherchée du piquage. Ici, le malfaiteur utilise un appareil électronique afin de prélever les données de la bande magnétique se trouvant au dos des cartes de paiement. Il y a, en gros, deux types d'appareils de pointe, un appareil portable et un appareil non portable. Les appareils portables sont ceux qui sont utilisés par les serveurs dans divers commerces, tels que les bars et les restaurants. Lorsque le client lui remet sa carte de paiement, le serveur peut la passer d'abord dans le lecteur de l'établissement, puis la passer à nouveau dans un lecteur portable qu'il remettra plus tard, avec toutes les données qu'il contient, à des acolytes. Un lecteur non portable peut être

---

[47] Voir, par exemple, *Beware phishing scam, TD Canada Trust warns customers*, CBC News, 31 juillet, 2007, consultable à http://www.cbc.ca/technology/story/2007/07/31/tech-td-phishing.html; U.S. Dep't of Justice, Alert About Hoax Emails, 30 janvier, 2008, consultable à http://www.usdoj.gov/hoaxemail.htm.

[48] Voir PRESIDENT'S IDENTITY THEFT TASK FORCE, COMBATTING IDENTITY THEFT: A STRATEGIC PLAN, aux pages 14 à 18, avril 2007, consultable à http://www.idtheft.gov; Sécurité Publique Canada, Avis public aux consommateurs : Vol d'identité, consultable à http://www.publicsafety.gc.ca/prg/le/bs/consumers-en.asp.

installé au-dessus de la fente d'un guichet automatique. Le client se prête sans le savoir à la manœuvre en introduisant sa carte dans la fente. Dans un premier temps, le lecteur installé par les malfaiteurs capte les données de la bande magnétique, puis le lecteur de l'établissement financier accepte la carte, reconnaît le NIP et complète la transaction. Pour déceler le NIP, les malfaiteurs installent parfois une caméra à sténopé près du clavier du guichet automatique afin que des complices puissent relever le NIP lorsque le client du guichet automatique le tape sur le clavier[49].

- **Vol de cartes ou de documents de paiement.** Il arrive souvent que des voleurs d'identité aient recours à des méthodes plus simples, notamment le vol de portefeuilles ou de sacs à main laissés dans une voiture ou dans un centre de conditionnement physique, ou les volent lors de l'expédition du courrier ou dans une boîte aux lettres. Le courrier contient parfois des offres de cartes de crédit préapprouvées que le voleur d'identité peut utiliser pour obtenir des cartes à d'autres noms. Ou bien, il peut modifier l'adresse du destinataire afin que la victime d'un vol d'identité ne reçoive jamais de courrier lui signalant qu'on lui avait envoyé une carte dont il n'avait pas fait la demande. Parfois, le courrier à expédier comprend un chèque ou un règlement de facture au moyen duquel le malfaiteur peut accéder au compte bancaire de sa victime.

b. Utilisation de renseignements signalétiques

Comme nous l'avons vu, il y a pour de nombreuses manières pour un malfaiteur d'utiliser des données personnelles, volées ou obtenues par fraude, pour commettre de nouvelles fraudes et dissimuler son identité véritable tout en rejetant les soupçons sur les victimes à qui il a subtilisé ces données. En effet, selon la Gendarmerie royale du Canada, à partir du moment où un voleur d'identité a obtenu les données personnelles de quelqu'un, il peut capter ses comptes financiers, ouvrir de nouveaux comptes bancaires, effectuer des transferts, demander des prêts, obtenir des cartes de crédit ou autres services, acheter des véhicules, voire se payer de belles vacances[50].

Un des phénomènes préoccupants de l'utilisation en ligne de données personnelles subtilisées est la création de« botnets » (c.-à-d. De réseaux d'ordinateurs dont les malfaiteurs ont pris le contrôle par piratage informatique ou l'installation de maliciels). À partir du moment où des malfaiteurs sont parvenus à constituer un botnet, ils peuvent utiliser les ordinateurs de ce réseau pour se livrer à toutes sortes d'activités et, par exemple, inonder les victimes éventuelles de pourriels, se livrer à des

---

[49] Voir, par exemple, *Police ask for help in card skimming case*, Owen Sound Sun-Times, 22 janvier, 2008, consultable à http://www.owensoundsuntimes.com/ArticleDisplay.aspx?e=869831&auth=Keith+Gilbert%2FSun+Media; *Regina bank customers hit by debit-card skimmers*, CBC News, 2 avril, 2007, consultable à http://www.cbc.ca/canada/saskatchewan/story/2007/04/02/regina-skimmers.html.

[50] Gendarmerie royale du Canada, consultable à http://www.rcmp-grc.gc.ca/scams/identity_theft_f.htm.

attaques de déni de service, propager des maliciels ou soutenir des offensives d'hameçonnage[51]. Plusieurs spécialistes de la sécurité informatique liés au SANS Institute, un des principaux organismes de formation en matière de sécurité informatique, ont conclu qu'en 2008 la sophistication et l'efficacité croissantes des botnets présenteront pour la sécurité informatique un des principaux risques[52].

[51] Voir, par exemple, Kelly Martin, *Stop the bots*, SecurityFocus, 18 avril, 2006, consultable en anglais uniquement à http://www.securityfocus.com/columnists/398/1.

[52] Voir SANS Institute, Press Release, 14 janvier, 2008, consultable en anglais uniquement à http://www.sans.org/press/top10menaces08.php.

Deuxième partie : Ripostes binationales aux fraudes par marketing de masse, 2004-2008

Depuis le rapport publié en 2003, le Canada et les États-Unis continuent à soutenir vigoureusement les ripostes binationales aux types de plus en plus variés de fraude par marketing de masse. Dans cette partie du rapport, nous nous pencherons sur les principaux changements apportés aux règles de droit et de procédure, à l'action des groupes de travail et des partenariats stratégiques mis en place pour lutter contre la fraude par marketing de masse, ainsi qu'aux mesures de prévention et de sensibilisation du public.

A. Règles de droit et de procédure

1. Le Canada

Les changements les plus importants qu'on se propose d'apporter à la législation canadienne susceptible d'avoir une incidence sur la fraude par marketing de masse, concernent le vol d'identité. Les problèmes que pose ce genre de délit devenant de plus en plus aigus en Amérique du Nord, Rob Nicholson, ministre de la Justice et procureur général du Canada a, en novembre 2007, déposé au Parlement un projet de loi faisant de l'obtention, de la possession ou du trafic de « renseignements identificateurs » sur une autre personne, un acte criminel lorsque ces données sont employées à des fins illicites.

Voici l'objet et les principales dispositions du projet de loi :

> L'utilisation à mauvais escient de renseignements relatifs à l'identité d'une autre personne, généralement appelée fraude d'identité, est visée par les infractions actuellement prévues au *Code criminel*, notamment la supposition de personne et la contrefaçon. Mais, les étapes préparatoires que constituent la collecte, la possession et le trafic de renseignements relatifs à l'identité ne sont généralement pas visées par les infractions actuelles. Le projet de loi vise la création de trois nouvelles infractions ciblant directement divers aspects du problème du vol d'identité, toutes assujetties à des peines maximales de cinq ans :
>
> - le fait d'obtenir et de posséder des renseignements relatifs à l'identité dans l'intention de les utiliser pour commettre certains crimes;
> - le fait de trafiquer des renseignements relatifs à l'identité en sachant que les renseignements doivent servir à la perpétration de certains crimes, ou en ne s'en souciant pas;
> - le fait de posséder ou de faire le trafic illégal de documents d'identité émis par le gouvernement.

D'autres modifications au *Code criminel* créeraient les nouvelles infractions de détournement frauduleux direct ou indirect du courrier, de possession d'une clé à courrier de Postes Canada contrefaite et de possession d'instruments de reproduction des renseignements de cartes de crédit, en plus de l'actuelle infraction de possession d'instruments de contrefaçon de cartes de crédit.
Les modifications prévoient également un nouveau pouvoir en vertu duquel un tribunal pourra ordonner à un contrevenant, dans le cadre de la peine prononcé, de dédommager la victime d'un vol d'identité ou d'une fraude d'identité si la victime a engagé des dépenses liées au rétablissement de son identité, telles que le coût des cartes et des documents de remplacement et les coûts liés à la correction de son dossier de crédit[53].

2. Les États-Unis

Parmi les mesures importantes prises aux États-Unis depuis 2003 dans le cadre de la lutte contre la fraude par marketing de masse, citons l'adoption du SAFEWEB Act[54]. Ce texte de loi confère à la Federal Trade Commission de nouveaux pouvoirs en matière de lutte contre les fraudes transfrontalières, et notamment :

- autorise la FTC à divulguer à des services de police étrangers, certains renseignements confidentiels ou protégés;

- autorise la FTC, sur demande écrite, à aider un service de police étranger dans ses enquêtes ou dans ses efforts en vue de faire aboutir les poursuites en cas d'infraction aux lois interdisant les pratiques commerciales frauduleuses ou trompeuses ou des pratiques analogues aux pratiques contraires aux lois administrées par la FTC, autres que les lois fédérales antitrust, sans qu'il soit nécessaire que la pratique en question soit effectivement contraire à la législation américaine;

- aux termes de ces nouvelles dispositions, la FTC doit 1) transmettre à l'Attorney General des États-Unis des preuves concernant la violation de la législation pénale fédérale par un citoyen, une société de personnes ou une entreprise, national ou étranger, et 2) en ce qui concerne les protocoles d'entente et les accords internationaux, veiller à ce que tout élément transmis par des autorités policières étrangères, puisse contribuer aux enquêtes ou aux poursuites visant des infractions au droit pénal américain, ou concourir à leur prévention;

---

[53] Ministère de la Justice, communiqué de presse, 21 novembre, 2007, consultable à http://www.justice.gc.ca/fr/news/nr/2007/doc_32178.html.

[54] Pub. L. No. 109-455, 120 Stat. 3372, 22 décembre 2006, consultable en anglais uniquement à http://www.ftc.gov/ogc/FTC_Act_IncorporatingUS_SAFE_WEB_Act.pdf

- la FTC est désormais autorisée à détacher certains de ses avocats pour aider l'Attorney General des États-Unis lors d'actions engagées devant les tribunaux étrangers, et de lui rembourser les honoraires versés à des avocats étrangers dans le cadre de procès dans des dossiers intéressant la FTC;

- la nouvelle loi précise les conditions dans lesquelles un dépositaire nommé par la FTC peut communiquer certains renseignements obligatoires ou confidentiels à des services policiers étrangers qui certifient que la confidentialité des renseignements en question sera préservée et que ces renseignements ne seront employés que dans le cadre de procédures officielles. Aux termes des nouvelles dispositions, tout renseignement transmis à la FTC par une source étrangère dans le cadre d'une enquête est dispensé des obligations de divulgation au titre du Freedom of Information Act;

- la FTC est désormais autorisée à 1) recourir provisoirement aux services d'employés de services officiels étrangers; 2) de détacher auprès de services étrangers des employés de la FTC; 3) au titre du Right to Financial Privacy Act de 1978, de communiquer des renseignements à certains organismes de régulation des marchés et du secteur financier; 4) d'accepter, de la part d'un service policier américain ou étranger, le remboursement de dépenses encourues par la FTC, ainsi que des cadeaux, des dons, des legs et des services dans la mesure où ils sont offerts volontairement et sans condition[55].

Ajoutons que les États-Unis, comme le Canada, tentent actuellement de faire adopter de nouvelles dispositions concernant le vol d'identité. Ainsi, en avril 2007, dans le cadre d'une stratégie nationale globale de lutte contre le vol d'identité[56], le Groupe de travail présidentiel sur le vol d'identité a recommandé que plusieurs modifications soient apportées au droit pénal fédéral, notamment :

- la modification des dispositions pénales fédérales en matière de restitution, afin que les victimes de vols d'identité puissent être indemnisées du temps nécessaire pour essayer de réparer les torts qui leur ont été causés;

- de modifier l'infraction fédérale réprimant le vol d'identité[57] ainsi que l'infraction réprimant le vol d'identité avec circonstances aggravantes[58] afin de faciliter les

---

[55] Voir Congressional Research Service, Summary of S. 1608, consultable à http://thomas.loc.gov/cgi-bin/bdquery/z?d109:SN01608 :@@@D&summ2=m&.

[56] Voir PRESIDENT'S IDENTITY THEFT TASK FORCE, COMBATTING IDENTITY THEFT: A STRATEGIC PLAN, 2008, consultable à http://www.idtheft.gov.

[57] 18 U.S.C. 1028(a)(7).

[58] 18 U.S.C. 1028A.

poursuites contre les voleurs d'identité qui détournent des renseignements appartenant à des entreprises ou autres organisations;

- de compléter la liste des infractions sous-jacentes en cas de vol d'identité avec circonstances aggravantes;

- la modification des dispositions pénales fédérales concernant le vol de données électroniques[59] en supprimant la disposition actuelle qui exige que les renseignements en question aient été volés au moyen de communications entre au moins deux États des États-Unis;

- l'imposition de sanctions aux créateurs et distributeurs de maliciels et d'enregistreurs de frappe en modifiant la loi fédérale sur le vol de données électroniques;

- de modifier la loi fédérale sur la cyberextorsion[60] afin d'en réprimer les diverses variantes[61].

Ces projets de modification législative sont actuellement à l'étude devant le Congrès des États-Unis.

B. Groupes de travail et partenariats stratégiques

Citons, parmi les éléments essentiels de la riposte binationale apportée au cours des dix dernières années à la fraude par marketing de masse, la création de groupes de travail et de partenariats stratégiques binationaux chargés de lutter contre ce véritable fléau. Depuis 1998, lorsqu'a été monté, à Montréal, le projet COLT, le premier de ces groupes de travail binationaux, les deux pays ont mis sur pied plusieurs groupes de travail et partenariats stratégiques régionaux : le projet COLT, l'Alliance stratégique de Toronto en Ontario, le Projet Emptor (Vancouver); le Alberta Partnership (Alberta); les provinces de l'Atlantique; et la Vancouver Strategic Alliance.

Chacun de ces groupes de travail et partenariats comprend des représentants des diverses organisations policières du Canada et des États-Unis. Citons, parmi les organismes représentés au sein d'au moins un de ces groupes de travail ou partenariats stratégiques, la British Columbia Business Practices and Consumer Protection Authority, le Service de police de la ville de Montréal, le Bureau de la concurrence (Canada), le Department of Homeland Security (Immigration & Customs Enforcement), le FBI, la

[59] 18 U.S.C. 1030.

[60] 18 U.S.C. 1030(a)(7).

[61] Voir PRESIDENT'S IDENTITY THEFT TASK FORCE, *supra*, note 53, aux pages 7 et 9.

FTC, le ministère de la Consommation et du Commerce de l'Ontario, la Police provinciale de l'Ontario, la Gendarmerie royale du Canada, la Sûreté du Québec, la police de Toronto, le United Kingdom Office of Fair Trading, le Service du U.S. Attorney (district central de Californie et district du sud de l'Illinois) et le U.S. Postal Inspection Service. Ces groupes de travail et partenariats stratégiques continuent à jouer un rôle essentiel dans la lutte contre la fraude transfrontalière par marketing de masse, non seulement en participant à l'action coordonnée des divers services (voir les pages qui suivent), mais également en participant aux mesures de sensibilisation du public et de prévention et, aussi, aux actions menées afin de contrer ces activités criminelles.

C. Systèmes de renseignement sur la consommation et de partage des renseignements

1. Canada

Au Canada, un des éléments clés du dispositif de renseignement sur la consommation et de partage des renseignements sur les fraudes par marketing de masse est PhoneBusters, le Centre d'appel antifraude du Canada. PhoneBusters est administré

> selon une entente tripartite entre la Police provinciale de l'Ontario, la Gendarmerie royale du Canada (GRC) et le Bureau de la concurrence Canada. PhoneBusters joue un rôle essentiel dans la sensibilisation du public au problème des arguments bidons utilisés dans le cadre des fraudes par télémarketing. Ce centre d'appel joue également un rôle essentiel dans la collecte et la diffusion des preuves et témoignages fournis par les victimes, des statistiques, de la documentation et des enregistrements, ces divers éléments étant mis à la disposition des services policiers d'autres pays[62].

PhoneBusters continue à servir à la fois les consommateurs souhaitant signaler des fraudes par télémarketing, des escroqueries liées au Nigeria ou des vols d'identité, et les organismes policiers canadiens et américains qui se servent de ces renseignements dans le cadre de leurs analyses et de leurs enquêtes.

Une autre structure très importante pour la lutte contre la fraude transfrontalière, y compris les fraudes perpétrées au moyen d'Internet, est le Système de signalement en direct des délits économiques (Centre RECOL) mis sur pied par la GRC. Le Centre RECOL est le fruit d'un partenariat intégré d'organismes policiers internationaux, fédéral et provinciaux, auquel participent également des organismes de réglementation ainsi que

[62] Le Centre d'appel antifraude du Canada, PhoneBusters, À propos de nous – consultable à http://www.phonebusters.com/francais/aboutus.html.

des entreprises privées pouvant légitimement prétendre recevoir des copies de plaintes visant des crimes économiques. Le Centre RECOL fournit en temps réel des données concernant les tendances actuelles en matière de fraude, et soutient en même temps les programmes de sensibilisation et de prévention des crimes économiques[63].

Un troisième système qui contribue très utilement à la coopération en matière de lutte contre la fraude transfrontalière est le réseau CANSHARE :

> Un système de partage des informations, basé sur Internet et conçu par les organismes d'application des lois sur la consommation aux niveaux fédéral et provincial pour leur propre usage. CANSHARE permet de réduire le dédoublement et d'accroître la vitesse et l'efficacité des échanges d'information entre juridictions. CANSHARE permet aux organismes d'application des lois sur la consommation d'affecter de manière plus efficace leurs ressources, ce qui entraîne une amélioration des programmes de protection des consommateurs. CANSHARE permet également aux diverses juridictions de surveiller et d'analyser les tendances du marché, d'identifier et de repérer les auteurs présumés de pratiques trompeuses, et d'émettre des avis et des mises en garde contre les diverses pratiques trompeuses[64].

Depuis son lancement en 1998, CANSHARE a été adopté par le gouvernement fédéral, par toutes les provinces ainsi que par deux territoires (le Yukon et les Territoires du Nord-Ouest)[65].

---

[63] Voir RECOL, consultable à https://recol.ca/intro.aspx?lang=fr.

[64] Comité des mesures en matière de consommation, Coopération en matière d'application des lois - Groupe de travail, consultable à http://http://cmcweb.ca/epic/site/cmc-cmc.nsf/fr/fe00030f.html.

[65] Voir Service Alberta, Press Release, consultable à http://www.servicealberta.gov.ab.ca/987.cfm.

2. Les États-Unis

Consumer Sentinel reste, aux États-Unis, le principal mécanisme national d'accueil des plaintes en matière de fraude à la consommation et de transmission aux organismes policiers, des données les concernant. Consumer Sentinel est une base de données entretenue depuis 1997 par la FTC et dans laquelle sont archivées toutes les données concernant les plaintes déposées par les consommateurs. Y sont recueillis des renseignements qui, en matière de fraude à la consommation et de vol d'identité, lui sont envoyés par la FTC ainsi que par 125 autres organisations. Les organismes d'application de la loi des États-Unis et des divers pays du monde y ont accès dans le cadre de leurs enquêtes. La base de données Sentinel comprend maintenant plus de 4,3 millions de plaintes[66]. Les données concernant les plaintes pour vol d'identité déposées auprès de la FTC peuvent être consultées par l'intermédiaire de la Identity Theft Data Clearinghouse de la FTC.

Pour les plaintes en matière de crimes commis par le truchement d'Internet, une autre composante essentielle de la lutte contre la fraude, tant du point de vue des services policiers que du public, est le Internet Crime Complaint Center (IC3). Il s'agit d'un partenariat entre le FBI et le National White Collar Crime Center, organisme privé à but non lucratif. Le IC3 recueille en ligne et analyse les plaintes du public et fait fonction de centre de consultation pour les organismes d'application de la loi des divers États des États-Unis ainsi que pour diverses autorités nationales et internationales. Le IC3 diffuse périodiquement, à l'intention du public, des avertissements concernant tel ou tel type de crime perpétré en ligne[67].

Citons la mise sur pied, depuis le rapport remis en 2003, d'une autre structure susceptible de contribuer très utilement aux enquêtes sur les fraudes par marketing de masse, la National Cyber-Forensics and Training Alliance (NCFTA). Il s'agit d'un organisme à but non lucratif qui sert d'instance neutre où peuvent être échangés discrètement d'importants renseignements confidentiels concernant les cyber-incidents, et où les moyens et les connaissances disponibles peuvent être partagés entre représentants des milieux industriels, universitaires et policiers[68]. Ce partenariat d'un genre unique a beaucoup aidé les divers organismes fédéraux chargés de l'application des lois à enquêter sur de complexes fraudes en ligne. À l'occasion de l'ouragan Katrina qui, en 2005, a dévasté une grande partie de la côte des États-Unis bordant le Golfe du Mexique, la NCFTA a puissamment contribué à l'analyse des vastes quantités de données

---

[66] Voir 2007 FTC, COMPLAINT DATA, *supra*, note 13, à la p. 2.

[67] Voir Internet Crime Complaint Center, consultable en anglais uniquement à http://www.ic3.gov/.

[68] Voir National Cyber-Forensics and Training Alliance, consultable en anglais uniquement à http://www.ncfta.net/default2.asp.

informatiques permettant d'identifier les sites Internet sollicitant frauduleusement des contributions aux fonds de solidarité censément destinés aux victimes de l'ouragan.

D. Résultats obtenus

1. La fraude par télémarketing

Depuis 2003, les groupes de travail et partenariats stratégiques binationaux ainsi que les divers organismes participants, ont engagé d'importantes poursuites, tant au pénal qu'au civil, contre les auteurs de fraudes transfrontalières par télémarketing. Peuvent être cités à cet égard, les affaires :

- *U.S. v. Bellini et al. (Acte d'accusation déposé le 19 décembre 2007).* Le 19 décembre 2007, 22 personnes ont été inculpées de fraude en raison de leur participation à un important stratagème de fraude transfrontalière par télémarketing basé à Montréal. Selon l'acte d'accusation, les membres de cette bande d'escrocs

  > auraient contacté les victimes, des personnes âgées pour la plupart, tentant de leur faire croire qu'elles avaient gagné de fortes sommes à la loterie ou dans un tirage au sort. Ces télévendeurs véreux auraient alors dit aux victimes que pour toucher leur prix, il leur fallait d'abord acquitter une taxe ou régler certains frais, voire, à au moins une occasion, verser l'argent nécessaire pour la location d'un fourgon blindé à bord duquel leur seraient livrés leurs gains. Selon l'acte d'accusation, aucune des victimes n'a en fait gagné quoi que ce soit, ni rien reçu de l'organisation de télémarketing. L'argent envoyé par les victimes, censément pour régler les frais, était simplement utilisé par les inculpés pour leurs menus plaisirs[69].

  C'est, semble-t-il, un des inculpés, l'organisateur et chef de l'organisation de télémarketing, qui s'était procuré l'équipement et les locaux nécessaires à l'opération. C'est lui qui se procurait la liste de personnes à berner comprenant des renseignements permettant de les identifier et de les contacter, et qui avait fourni à ses acolytes des téléphones portables, assuré la formation des nouveaux membres de l'organisation et réuni l'équipe de gens chargés de démarcher les victimes en puissance, organisé la réception des sommes versées par les victimes, converti en dollars canadiens les chèques envoyés par des victimes américaines et réparti l'argent entre les membres de la bande. D'autres membres de la bande étaient, semble-t-il, chargés de contacter les victimes par téléphone. Cinq des inculpés

[69] U.S. Attorney's Office, Central District of California, Press Release, 19 décembre, 2007, consultable en anglais uniquement à http://www.usdoj.gov/usao/cac/pressroom/pr2007/163.html.

auraient géré des commerces de transfert monétaire, en l'occurrence des succursales de Western Union et de MoneyGram, auxquelles il avait été demandé à certaines victimes d'effectuer un virement télégraphique. Étant donné leurs contacts au sein de ces succursales, les membres de l'organisation pouvaient dissimuler leur identité, demandant aux victimes de transférer l'argent à des identités fictives[70].

Si les membres de cette bande ont pu être inculpés, c'est en raison d'une enquête de huit mois menée dans le cadre du projet COLT. Dans le cadre de cette enquête, environ 200 policiers ont effectué, au Canada, une cinquantaine de perquisitions, essentiellement dans la région de Montréal et le FTC, aux États-Unis, a contacté près de 400 consommateurs afin d'obtenir des déclaration auprès des victimes. Les autorités canadiennes ont, à l'époque, arrêté 20 des 22 personnes qui devaient ultérieurement être inculpées aux États-Unis. Quatre-vingt pour cent des transactions auraient été effectuées par l'intermédiaire des centres de virement télégraphique installés à Montréal. D'après les autorités, cette bande, dont les activités consistaient essentiellement à monter des escroqueries à la loterie et à faire des offres frauduleuses de prêts ou de bourses, récoltait, depuis 2003, environ cinq à dix millions de dollars par an[71].

- *U.S. v. Okuomose (arrestation en date du 6 novembre 2007)/FTC v. B.C. Ltd. 0763496, d.b.a. Cash Corner Services, Inc. Et al., Civil Action No. C07-1755 RSM (injonction préliminaire en date du 13 novembre 2007)*. Dans le cadre de cette enquête conjointe menée par le projet EMPTOR, un résident de Colombie-Britannique a été arrêté par des agents de la GRC en vertu d'un mandat d'arrestation provisoire décerné au vu d'une plainte pénale déposée auprès de la U.S. District Court de Los Angeles. L'inculpé était recherché en raison de sa participation à une escroquerie à la loterie. Il opérait sous la raison sociale de « Cash Corner Services » à partir de Colombie-Britannique et choisissait ses victimes parmi des personnes habitant les États-Unis. Voici, selon les détails de la plainte déposée, comment il opérait :

  > Il envoyait à ses éventuelles victimes, une lettre dans laquelle il leur annonçait qu'elles avaient gagné à la loterie, mais que pour toucher leurs gains, il leur fallait au préalable acquitter certains droits. Selon l'accusation, la lettre était accompagnée d'un chèque falsifié devant permettre à la victime d'acquitter les droits qui lui étaient réclamés. Le numéro de téléphone indiqué dans ce courrier permettait à la

[70] Voir *id*.

[71] Voir Gendarmerie royale du Canada, Division « C », communiqué de presse, 4 janvier 2008, consultable à http://www.rcmp-grc.gc.ca/qc/comm/2008/01/080104_f.htm.

> victime de contacter des télévendeurs qui lui confirmaient qu'elle avait effectivement gagné à la loterie mais qu'il lui fallait, pour toucher son argent, acquitter certains droits. Certaines victimes ne recevaient pas de lettre mais seulement un coup de téléphone qui, selon l'accusation, les persuadait d'envoyer de l'argent à l'organisation responsable de la loterie. Les droits qu'il était demandé aux victimes d'acquitter allaient de quelques milliers de dollars à 24 000 $. Après avoir envoyé l'argent, la victime tentait d'encaisser le chèque qui lui avait été envoyé, mais s'apercevait, bien sûr, que ce chèque ne valait rien. Jusqu'ici, aucunes des victimes interviewées n'a reçu la moindre partie de l'argent qui leur avait été promis[72].

Dans des procès civils engagés parallèlement, la FTC a poursuivi l'inculpé, de même qu'un proche de celui-ci, Cash Corner Services et une autre entreprise canadienne, invoquant la violation du Federal Trade Commission Act et de la FTC Telemarketing Sales Rule, et obtenant à leur encontre une injonction préliminaire. La British Columbia Business Practices and Consumer Protection Authority a, pour sa part, engagé une action civile contre les responsables, demandant au tribunal le gel de leurs avoirs au Canada[73].

Précisons que le personnel du FTC a porté assistance aux autorités canadiennes en ayant recours aux dispositions du SAFEWEB Act américain pour communiqué leur communiquer des renseignements qu'elle avait recueillis dans le cadre de son enquête, afin que les enquêteurs canadiens puissent en faire aussi usage[74].

- *U.S. v. Porcelli (condamnation prononcée le 29 octobre 2007).* Le 29 octobre 2007, l'inculpé a été condamné à 13 ans d'emprisonnement pour sa participation à une fraude par télémarketing ayant permis de subtiliser environ 12 millions de dollars à des individus habitant diverses régions des États-Unis. Ce stratagème, qui offrait frauduleusement des cartes de crédit à des personnes à qui des établissements financiers légitimes avaient précédemment refusé d'en accorder, était basé en Floride et dans l'Utah et avait recours à des centres d'appels sortants de sept États des États-Unis, à des centres d'appels sortants situés à la Grenade, à

---

[72] FBI, communiqué de presse, 6 novembre 2007, disponible seulement en anglais http://losangeles.fbi.gov/pressrel/2007/la110607a.htm.

[73] Voir FTC, communiqué de presse, 19 novembre 2007, disponible seulement en anglais http://www.ftc.gov/opa/2007/11/cashcorner.shtm.

[74] Voir *id.*

Sainte-Lucie et à Saint-Vincent, à un centre d'appels sortants situé à Toronto (Canada) et à des centres d'appels sortants situés en Inde[75].

- *Perquisitions dans le cadre d'une enquête sur des fraudes par marketing de masse (Montréal, le 9 octobre 2007).* Le 9 octobre 2007, des agents du projet COLT ont effectué des perquisitions à Montréal, dans le cadre d'une enquête sur une bande d'escrocs se livrant à des fraudes par télémarketing qui avaient, semble-t-il, fait 1 500 victimes. Les téléphonistes de la bande avaient recours à divers types de baratins, y compris 1) la vente de trousses de secours, aux entreprises, en se faisant passer pour des représentants d'un organisme sanitaire fédéral chargé d'appliquer la réglementation exigeant la présence d'une telle trousse dans toutes les entreprises; 2) la vente de papeterie en se faisant passer pour un fournisseur légitime; et 3) la vente, aux entreprises, d'une inscription dans un bottin d'entreprises alors que les bottins livrés ne comprenaient pas les inscriptions promises et payées. Les victimes de ce genre de stratagème étaient en général des petites et moyennes entreprises du Canada, des États-Unis et d'Europe[76].

- *U.S. v. Kimoto (acte d'accusation déposé le 20 juin 2007).* Le 20 juin 2007, un résident de St. George (Utah) et de Las Vegas, a été inculpé de diverses infractions fédérales liées à une combine frauduleuse par télémarketing offrant une carte de crédit à des personnes qui s'en étaient déjà vu refuser une. Selon l'acte d'accusation, ce stratagème était basé dans l'Utah et employait tout un réseau de centres d'appels sortants que l'inculpé avait organisé dans sept États des États-Unis, ainsi que des centres d'appels sortants installés dans les Caraïbes, notamment à la Grenade, à Sainte-Lucie et à Saint-Vincent, un centre d'appels sortants installé à Toronto (Canada) ainsi que divers centres d'appels situés en Inde. Selon l'acte d'accusation, cette escroquerie avait fait plus de 300 000 victimes parmi les consommateurs des États-Unis, la fraude s'élevant à quelque 43 millions de dollars[77]. L'inculpé et ses sociétés avaient déjà fait l'objet d'une sanction imposée par la FTC qui avait obtenu des tribunaux qu'ils

[75] Voir U.S. Attorney's Office, Southern District of Illinois, communiqué de presse, 29 octobre 2007, consultable en anglais uniquement à http://www.usdoj.gov/usao/ils/press/2007/Oct/10292007_Porcelli_press%20release.htm.

[76] Voir Gendarmerie royale du Canada, Division C, communiqué de presse, 9 octobre 2007, consultable à http://www.rcmp-grc.gc.ca/qc/comm/archives/2007/10/071009_f.htm.

[77] Voir U.S. Attorney's Office, Southern District of Illinois, communiqué de presse, 20 juin 2007, disponible seulement en anglais http://www.usdoj.gov/usao/ils/press/2007/Jun/06202007_Kimoto%20press%20release.htm.

prononcent une mise sous séquestre, et condamnent une des entreprises à reverser 106 millions de dollars[78].

- *U.S. v. Brown and Love (plaidoyer de culpabilité en date du 29 mars 2007)*. En l'occurrence, deux résidents de Las Vegas ont plaidé coupable aux accusations portées contre eux en vertu des dispositions pénales fédérales, pour blanchiment du produit d'opérations illicites de télémarketing menées au Canada. Selon les services du U.S. Attorney's Office chargé du dossier, en avril 2004, l'une des inculpées avait rencontré, par Internet, une personne se présentant comme « Missy Young », habitant en Ontario (Canada). « Young » (un nom d'emprunt) a alors dit à l'inculpée qu'avec plusieurs autres personnes, elle faisait, au Canada, du télémarketing et aurait besoin de trouver des gens habitant les États-Unis afin d'ouvrir des comptes en banque susceptibles d'accueillir le produit de ses opérations de télémarketing et de les transférer au Canada. Entre juin 2004 et janvier 2005, la première inculpée a ouvert sept comptes en banque auprès de divers établissements bancaires, utilisant pour cela le nom de plusieurs entreprises différentes. Cette inculpée a obtenu que l'autre ouvre deux comptes en banque de plus. Au cours de cette période, par des virements télégraphiques à des comptes en banque contrôlés aux États-Unis et au Canada par les télévendeurs, la première inculpée a transféré environ 802 000 $ en argent américain. Les télévendeurs ont également eu accès à ces comptes en banque au moyen de retraits effectués à des guichets automatiques aux États-Unis et au Canada. Au cours de cette même période, et de la même manière, la seconde inculpée a, à partir des comptes en banque qu'elle avait ouverts, transférer environ 630 700 $ US aux télévendeurs installés au Canada.

  Il s'agissait, par le truchement de ces opérations de télémarketing menées à partir du Canada, de soutirer de l'argent aux victimes par des mensonges et des faux-semblants. Des télévendeurs opérant au Canada auraient contacté des citoyens des États-Unis, leur offrant de leur vendre un produit ou un service d'une valeur d'environ 300 $. Prétextant cette supposée vente, les télévendeurs au Canada établissaient un mandat ou un chèque « préautorisé » le déposant dans un des comptes en banque ouverts par les inculpées. Les renseignements bancaires et personnels figurant sur les chèques préautorisés comprenaient le nom, l'adresse, le numéro de compte et le numéro d'acheminement de la banque, ces renseignements ayant été obtenus frauduleusement, car une forte proportion des chèques en

[78] Voir Final Monetary Judgment As To Defendants Kyle Kimoto and Assail, Inc., *FTC v. Assail*, Civil Action No. W-03-CA-007, W.D. Tex., 24 septembre 2004, consultable en anglais uniquement à http://www.ftc.gov/os/caselist/assail/050124kimoto.pdf.

question avaient été remplis sans que la personne frauduleusement désignée comme l'« acheteur » soit au courant ou ait donné son autorisation[79].

2. La fraude par Internet

Voici quelques exemples de poursuites menées dans des dossiers de fraude transfrontalière par Internet :

- *U.S. v. Hendricks (condamnation prononcée le 25 février 2007)*. Le 25 février 2007, un habitant de la Floride a été condamné à six ans de prison après avoir plaidé coupable à plusieurs infractions à la législation pénale des États-Unis, en raison du rôle qu'il avait joué en tant que dirigeant d'un cabinet d'investissements frauduleux qui avait soutiré environ 13 millions de dollars à plus de 1 500 victimes résidant aux États-Unis et au Canada. L'inculpé a reconnu avoir, dans le cadre d'une entreprise qu'il avait constituée avec un autre individu, Pacific Achievements International (PAI), et par des fausses promesses et déclarations, sollicité des fonds à investir, en général par le truchement d'Internet. Il avait faussement fait valoir aux investisseurs que la PAI était une entreprise de marketing par réseau, leur promettant que s'ils plaçaient leur argent chez PAI, ils toucheraient une prime initiale, puis d'importants bénéfices.

  Se fiant à ces fausses promesses et à ces arguments mensongers, les investisseurs ont versé plus de 13 millions de dollars sur les comptes en banque de la PAI, dans les États de l'Oregon, de Washington et de Floride, ces comptes étant contrôlés par l'inculpé et un autre individu. L'inculpé et un autre promoteur de la PAI ont détourné plus de deux millions de dollars de l'argent de la PAI pour entretenir un luxueux mode de vie, consacrant notamment 1,6 million de dollars à l'achat de résidences en Floride et dans l'État de Washington. Sachant pertinemment que la PAI n'était pas génératrice de revenus, l'inculpé et un autre promoteur de l'entreprise ont tenté de récupérer les sommes détournées en investissant les fonds de la PAI dans des combines risquées qu'ils croyaient très rentables, à Beyrouth (Liban) ainsi qu'aux Bahamas, au Nevada et au Texas. Du fait de ces autres combines, ils ont fini par perdre 2,7 millions de dollars appartenant à la PAI. Les inculpés ont plaidé coupable. Ils étaient accusés de complot en vue de fraudes postales et télégraphiques, et de non-déclaration de revenu au fisc américain[80].

---

[79] Voir U.S. Attorney's Office, Western District of New York, communiqué de presse, 2 avril, 2007, consultable en anglais uniquement à http://www.usdoj.gov/usao/nyw/press/press_releases/BROWNANDLOVEPRESS.pdf.

[80] Voir U.S. Attorney's Office, District of Oregon, communiqué de presse, 25 février, 2007, consultable à http://portland.fbi.gov/dojpressrel/2007/investmentscheme022507.htm; U.S. Attorney's Office, District of Oregon, communiqué de presse, 24 octobre 2006, consultable à

- *U.S. v. Kraser (condamnation prononcée le 7 mai 2006).* L'inculpé a été condamné à 21 mois de prison pour avoir frauduleusement sollicité des dons charitables dont il prétendait qu'ils serviraient à secourir les victimes de l'ouragan Katrina. Selon l'acte d'accusation, l'inculpé a, au cours de ses contacts sur Internet, ainsi que sur un site Internet dont l'adresse était www.AirKatrina.com, faussement fait valoir qu'en tant que pilote, il assurait alors des vols vers la Louisiane afin d'apporter des fournitures médicales aux zones les plus touchées par l'ouragan, et d'en évacuer les enfants et autres personnes en très mauvaise santé. Il prétendait également avoir recruté un groupe de pilotes de la Floride pour l'aider dans cette opération de secours[81]. En deux jours, l'inculpé a subtilisé environ 40 000 $ à 40 personnes habitant les États-Unis, le Canada, le Mexique, l'Europe et Hong Kong, une des victimes lui envoyant 20 000 $[82].

3. Escroqueries ayant pour origine le Nigeria

Nous avons vu que les consommateurs sont, tant au Canada qu'aux États-Unis, de plus en plus menacés par des escroqueries liées au Nigeria. Voici quelques exemples récents de ripostes aux combines frauduleuses nigérianes :

- *U.S. v. Anisiobi et al. (plaidoyers de culpabilité en date du 30 janvier 2008).* Le 30 janvier 2008, trois inculpés, extradés des Pays-Bas vers les États-Unis en raison de leur participation à une bande d'escrocs nigérians basée à Amsterdam, ont plaidé coupable à diverses accusations de complot, de fraude télégraphique et de fraude postale. Selon l'acte d'accusation et une plainte déposée plus tôt à leur encontre,

> Les inculpés ont envoyé des courriels à des milliers de victimes éventuelles, tentant de leur faire croire qu'ils contrôlaient des millions de dollars placés à l'étranger. Afin de dissimuler leurs identités, les inculpés ont employé des faux-noms, de faux numéros de téléphone et de fausses adresses électroniques. Dans le cadre d'un de leurs stratagèmes, les inculpés ont envoyé des courriels censés émaner d'une personne atteinte d'un cancer de la gorge en phase terminale et qui voulait qu'on l'aide à distribuer 55 millions de dollars à diverses oeuvres de charité. En échange de l'aide que lui fournirait la victime, les inculpés offraient de verser

---

http://portland.fbi.gov/dojpressrel/2006/investmentfrau102406.htm.

[81] Voir U.S. Attorney's Office, Southern District of Florida, communiqué de presse, 8 mai 2006, consultable à http://miami.fbi.gov/dojpressrel/pressrel06/mm050806.htm.

[82] Voir FBI, Busted for Katrina Fraud, 21 octobre, 2005, consultable à http://www.fbi.gov/page2/oct05/katrinaescam102105.htm.

> une commission de 20 p. 100, soit à la victime elle-même soit à une œuvre charitable qu'elle aurait désignée. Afin de rendre leur stratagème plus crédible, les inculpés envoyaient aux victimes éventuelles divers faux documents, y compris une lettre d'autorisation et un certificat de dépôt attestant la disponibilité des fonds en question, ainsi que des photographies de la personne censée souffrir d'un cancer de la gorge. Un des inculpés aurait téléphoné aux victimes, déguisant sa voix afin de leur faire croire qu'il était atteint d'un cancer de la gorge.
>
> Après avoir acquis la confiance de leurs victimes, les inculpés leur demandaient de transmettre par virement télégraphique une somme censée correspondre à certains frais devant être acquittés à l'avance, notamment pour payer les honoraires d'avocat, certaines taxes ainsi que la délivrance de divers documents. En échange, les victimes ne recevaient absolument rien. Dans une variante de ce stratagème, si la victime affirmait ne pas avoir les moyens d'acquitter les droits qui lui étaient demandés, les inculpés leur envoyaient, pour compenser le paiement des frais en question, de faux chèques de la part, disait-il, du malade. De nombreuses victimes ont déposé ces chèques, effectuant en même temps un retrait afin d'envoyer par virement télégraphique, la somme qui leur était réclamée. Les victimes ont essuyé de sérieuses pertes lorsque les chèques n'ont pas été honorés[83].

- *R. v. Anigozie et al. (Ontario, arrestation en date du 2 novembre 2007).* À l'issue de cette enquête, trois résidents de l'Ontario ont été arrêtés pour production et multidiffusion de faux chèques à travers l'Amérique du Nord. Les enquêteurs se sont principalement intéressés au laboratoire où étaient fabriqués ces chèques falsifiés. Il semblerait que ces faux chèques, et la documentation attestant leur authenticité, devaient servir à des fraudes à la charité, à la loterie ou aux prêts personnels. La police a également exécuté cinq mandats de perquisition, saisi plusieurs systèmes informatiques, imprimantes, scanners, de faux dollars américains ainsi que des milliers de chèques à diverses étapes du processus de production[84].

- *U.S. v. Roberts (condamnation prononcée en janvier 2006).* En l'occurrence, l'inculpé a été condamné à 18 mois d'emprisonnement pour sa participation à une escroquerie comportant la distribution de faux chèques. On a trouvé chez lui, lors

---

[83] Voir U.S. Attorney's Office, Eastern District of New York, communiqué de presse, 30 janvier 2008, consultable à http://www.usdoj.gov/usao/nye/pr/2008/2008jan30.html.

[84] Voir Police provinciale de l'Ontario, communiqué de presse, 2 novembre 2007.

de son arrestation, des faux chèques et des faux mandats d'un montant de plus de 680 000 $. Il a plus tard affirmé aux agents de la force publique qu'il avait rencontré, sur Internet, un certain « John », que ce « John » lui avait envoyé des faux chèques et des mandats falsifiés, ainsi que le montant des frais d'affranchissement pour expédition par UPS et des instructions quant à la manière de distribuer les chèques aux personnes choisies comme cibles[85].

4. Vol d'identité

Voici quelques exemples d'actions répressives exercées depuis 2003 contre des malfaiteurs se livrant à des vols d'identité impliquant une activité transfrontalière :

- *U.S. v. Hardiman (condamnation prononcée le 12 septembre 2007)*. Le 12 septembre 2007, un résident de Toronto a été condamné à deux ans d'emprisonnement pour vol d'identité avec circonstances aggravantes. L'inculpé, qui se livrait au trafic de cartes de crédit contrefaites avait, par le truchement d'Internet, vendu de fausses cartes de crédit et de faux permis de conduire. Les fausses cartes de crédit portaient un numéro correspondant à des comptes authentiques auprès d'entreprises de services financiers, y compris Wachovia, Visa et American Express. Les faux permis de conduire fabriqués par l'inculpé portaient le numéro du permis de conduire de personnes vivant au Canada, dans la province censée avoir délivré le permis de conduire en question. L'enquête a été menée conjointement par le U.S. Secret Service et la Police de Toronto[86].

- *U.S. v. Ciocan and Pasca (acte d'accusation en date du 8 mai 2007).* En l'occurrence, deux personnes de nationalité roumaine vivant au Canada ont été accusées, en vertu des lois fédérales, de complot, de fraude bancaire et de vol d'identité avec circonstances aggravantes en raison de leur participation à un stratagème de vol d'identité dans le cadre duquel les malfaiteurs s'emparaient furtivement, à des guichets automatiques, des renseignements identificateurs des clients d'une banque. Selon l'accusation, les inculpés auraient pris part à une arnaque dans le cadre de laquelle les complices installaient, sur des guichets automatiques, des lecteurs de carte permettant de subtiliser le numéro de compte et autres renseignements figurant sur les cartes, sans que l'utilisateur ne s'en aperçoive.

---

[85] Voir U.S. Attorney's Office, Southern District of West Virginia, communiqué de presse, 11 janvier 2006), consultable à http://www.usdoj.gov/usao.wvs/press_releases/2006/jan06/011106.html.

[86] Voir U.S. Attorney's Office, Western District of New York, communiqué de presse, 12 septembre 2007), consultable à http://www.usdoj.gov/usao/nyw/press/press_releases/HardimanSentencing.pdf.

> Les membres de la bande se sont également procuré frauduleusement les numéros d'identité personnelle correspondant aux cartes. Les malfaiteurs ont alors utilisé les renseignements prélevés sur les cartes bancaires pour fabriquer de fausses cartes. Les inculpés se sont alors rendus d'une ville à l'autre, utilisant pour retirer des fonds de divers guichets automatiques, les cartes contrefaites et les numéros d'identité personnelle subtilisés[87].

- *Accusations pour vol d'identité par Internet (Ontario, accusations portées en mars 2006).* Dans cette affaire, la Police d'Ottawa a découvert un stratagème de vol d'identité par Internet visant les candidats à des postes affichés en ligne. Les membres de la bande auraient annoncé à leurs éventuelles victimes qu'on avait retenu leur candidature à un poste auquel était rattaché un salaire annuel de 70 000 $. Les arnaqueurs demandaient alors à leurs victimes de remplir une demande et de la leur transmettre accompagnée de la somme de 20 $ pour les frais de constitution de dossier. Les malfaiteurs utilisaient les renseignements personnels qui leur étaient ainsi transmis pour demander, au nom de leurs victimes, des cartes de crédit, des papiers d'identité et des cartes d'assurance sociale. Deux des suspects ont été arrêtés après que, exécutant un mandat de perquisition à l'une de leurs résidences, la Police d'Ottawa a saisi une soixantaine de cartes de crédit, de cartes d'assurance sociale et de permis de conduire ontariens et québécois. Selon les autorités, les suspects se seraient livrés à cette escroquerie depuis 2002[88].

E. Mesures de prévention et de sensibilisation du public

Depuis 2003, les autorités policières du Canada et des États-Unis s'attachent, par divers moyens, à améliorer l'information du public en matière de fraude par marketing de masse. Citons, à cet égard :

- **La perturbation des activités criminelles.** Vers la fin de 2007, le projet COLT, ayant appris que certaines enveloppes à destination de diverses adresses aux États-Unis, comprenaient des documents de marketing frauduleux, est parvenu, après un

---

[87] U.S. Attorney's Office, Western District of Pennsylvania, communiqué de presse, 9 octobre 2007), consultable à http://pittsburgh.fbi.gov/dojpressrel/2007/identitytheft050907.htm.

[88] Voir *Two charged in Internet-based identity theft scam*, ctv.ca, 9 mars 2006, consultable à http://www.ctv.ca/servlet/ArticleNews/story/CTVNews/20060308/idtheft_scam_060308?s_name=&no_ads=.

mois de surveillance, à découvrir plus de 50 000 lettres frauduleuses adressées surtout à des résidents des États-Unis, mais aussi à certains résidents canadiens. Cette tentative de fraude portait sur un total de presque 195 millions de dollars. Les lettres en question comprenaient de faux chèques pour des sommes allant de 2 000 à 5 000 $. Les résultats obtenus dans le cadre de cette opération ont fourni à la GRC l'occasion de mettre le public en garde contre les fraudes qu'elle avait découvertes[89].

Certaines initiatives destinées à perturber l'action des malfaiteurs se livrant à des fraudes par marketing de masse tournent parfois à l'avantage des victimes. Ainsi, depuis 1998, le projet COLT a permis de récupérer, à l'intention des victimes, plus de 20 millions de dollars.

- **Avertissements au public.** Dans les deux pays, plusieurs organismes ont émis des avertissements mettant le public en garde contre certains types de fraude par marketing de masse, notamment l'emploi de faux chèques et de faux mandats[90] dans le cadre de combines frauduleuses et de pourriels émanant prétendument de divers services d'application de la loi[91].

[89] *Voir* Gendarmerie royal du Canada, Division « C », communiqué de presse, 18 décembre 2007), consultable à http://www.rcmp-grc.gc.ca/qc/comm/archives/2007/12/071218_f.htm.

[90] Voir Public Safety and Emergency Preparedness Canada and U.S. Dep't of Justice, Public Advisory: Special Report on Counterfeit Checks and Money Orders, consultable à http://www.usdoj.gov/opa/public_advisory_counterfeit.pdf.

[91] Voir, par exemple, U.S. Secret Service, FRAUDULENT SPAM E-MAIL CLAIMING TO BE FROM THE U.S. SECRET SERVICE, 26 janvier 2007, consultable à http://www.secretservice.gov/fraud_email_advisory.shtml.

- **Campagnes de sensibilisation du public et de publicité.** En 2007, la GRC et les autorités policières de certains pays, autres que d'Amérique du Nord, ont pris part à une initiative du U.S. Postal Inspection Service destinée à avertir le public des risques d'escroquerie au moyen de faux chèques. Le volet pédagogique de cette initiative comprend des messages publicitaires d'intérêt public à la télévision et dans la presse écrite ainsi que sur un site Internet, créé par le Ligue nationale des consommateurs des États-Unis, sur lequel sont publiées d'autres informations à caractère didactique[92]. Cette initiative comprend des mesures prises conjointement par des organismes du secteur public et du secteur privé, y compris sept des principales entreprises de services financiers, des associations et la Publishers Clearing House, toutes contribuant à la promotion de cette campagne de sensibilisation[93].

  La FTC a pris de nombreuses mesures en vue d'informer le public des risques de fraude par marketing de masse. Ainsi, en 2006, la FTC et la Food and Drug Administration des États-Unis, en collaboration avec des organismes gouvernementaux du Canada et du Mexique, ont lancé une grande campagne contre les publicités trompeuses et la vente de produits prétendument censés guérir ou traiter le diabète. En date du mois d'octobre 2006, dans le cadre de cette campagne menée conjointement, environ 180 lettres d'avertissement et autres mises en garde ont été publiées sur des sites Internet dans les trois pays[94]. En 2006, encore, la FTC a organisé, à New York, à l'intention de la population hispanophone, un Forum sur la prévention de la fraude. La FTC a annoncé, dans le cadre de ce forum, la publication de nouveaux matériaux didactiques à l'intention des consommateurs, et la création de nouveaux partenariats pour organiser des campagnes de sensibilisation dans les écoles de New York, ainsi que les résultats d'un Hispanic Multi-Media Surf, organisé par la FTC et 60 partenaires aux États-Unis et en Amérique latine[95].

  Au Canada, le projet COLT a mis sur pied, dans la région de Montréal, une campagne d'information s'adressant aux étudiants susceptibles d'être recrutés pour travailler dans des "chaufferies" en télémarketing. Au moyen d'annonces et de dépliants, le Project COLT mettait les employés potentiels en garde des dangers

---

[92] Voir fakechecks.org, consultable à http://www.fakechecks.org/.

[93] Voir fakechecks.org, About Us, consultable à http://www.fakechecks.org/links.html.

[94] Voir Food and Drug Administration, communiqué de presse, 19 octobre, 2006, consultable à http://www.fda.gov/bbs/topics/NEWS/2006/NEW01494.html.

[95] Voir FTC, communiqué de presse, 27 septembre, 2006, consultable à http://www.ftc.gov/opa/2006/09/nyworkshop.shtm.

qu'ils peuvent encourir en travaillant dans ce genre d'entreprise frauduleuse. Le Projet COLT encourageait aussi les étudiants à rapporter les activités douteuses aux forces de l'ordre.

En 2005, grâce aux contributions provenant du DOJ (département de la justice), du "United States Postal Inspection Service", d'autres agences fédérales et de plusieurs groupes du secteur privé, le FTC a lancé le site web interactif "On Guard Online" (www.onguardonline.gov) lequel fourni des conseils aux consommateurs pour les aider à mieux se protéger contre diverses fraudes par marketing de masse, incluant le vol d'identié, "l'hameçonnage", les logiciels espions, les pourriels frauduleux et le VoIP

Plus récemment, en février 2008, le U.S. Postal Inspection Service a lancé une campagne nationale de sensibilisation de la population au vol d'identité. Dans le cadre de cette campagne, le Postmaster General, principal responsable des Postes aux États-Unis, a envoyé 121 millions de lettres destinées à tous les ménages des États-Unis et comprenant une brochure de la FTC sur le vol d'identité.

Mars est le mois de la prévention de la fraude. Au Canada, en mars, le Forum sur la prévention de la fraude[96], sous l'égide du Bureau de la concurrence du Canada, mène une campagne concertée de sensibilisation à la fraude. Par tout un éventail d'activités et de moyens de communication, les plus de 100 organisations membres du Forum, tant du secteur privé que du secteur public, envoient des millions de messages pour alerte et sensibiliser le public aux risques de fraude.

[96] Voir Campagne 2008 du Mois de la prévention de la fraude et liste des membres partenaires du Forum sur la prévention de la Fraude, consultable à http://www.bureaudelaconcurrence.gc.ca/epic/site/cb-bc.nsf/fr/h_00122f.html

Troisième partie : La constance dans la lutte contre la fraude par marketing de masse - L'affinage du plan d'action binational

Depuis la remise du rapport de 2003, le Canada et les États-Unis n'ont cessé de renforcer la coopération entre les deux pays afin de lutter plus efficacement contre les fraudes transfrontalières, et plus particulièrement la fraude par marketing de masse. Cette collaboration des services des deux pays a permis de créer de nouveaux groupes de travail conjoints et partenariats stratégiques. Les enquêtes entreprises dans le cadre de cette action conjointe ont permis de sanctionner les auteurs de grosses combines frauduleuses employant des techniques de marketing de masse.

L'expérience acquise par les deux pays depuis 2003, dans le cadre de cette lutte contre la fraude par marketing de masse, démontre l'importance essentielle que revêt la collaboration et la mise en commun des moyens et des informations. Les services de police, le procureurs publics et les autorités réglementaires des deux pays vont devoir s'entendre sur les nouvelles mesures à prendre afin de rendre encore plus efficace cette lutte contre les stratagèmes frauduleux transfrontaliers.

Afin d'assurer la cohérence de l'action répressive menée conjointement par les deux pays, le rapport 2003 avait défini un plan d'action comprenant d'importantes mesures pour renforcer les moyens de lutte binationaux contre les principaux types de fraude transfrontalière touchant les deux pays. Ce plan d'action faisait état des considérations stratégiques et opérationnelles intéressant les enquêtes, les poursuites, la sensibilisation du public et la prévention des fraudes transfrontalières.

A. Le plan d'action binational de lutte contre la fraude transfrontalière

Le plan d'action élaboré en 2003 comprenait 12 points groupés en cinq rubriques. Dans cette partie du rapport, nous évoquerons les mesures qui ont été prises depuis, ainsi que celles qui vont devoir l'être, afin d'assurer la mise en œuvre des recommandations formulées à l'époque. Il y a lieu, par ailleurs, de faire une recommandation de plus afin de tenir compte de l'évolution depuis lors du phénomène de la fraude par marketing de masse.

1. Les stratégies

1) ***Les deux pays devront confronter leurs stratégies respectives de lutte contre la fraude transfrontalière par télémarketing et les mettre en accord afin de mieux combattre les nouvelles manifestations de la fraude par télémarketing.***

Depuis le rapport 2003, des membres des groupes de travail nationaux mis sur pied dans nos deux pays, y compris le présent sous-groupe et le Groupe de travail canadien sur la stratégie de prévention des fraudes par marketing de masse, ont approfondi leurs discussions sur le cadre stratégique actuel et précisé les domaines où il y aurait lieu d'harmoniser plus avant les stratégies adoptées. Le Groupe de travail sur la stratégie de prévention des fraudes par marketing de masse ayant achevé ses travaux d'élaboration d'une stratégie nationale, les organismes intéressés des deux pays devraient maintenant être en mesure de coordonner encore plus étroitement leurs stratégies respectives.

2) ***Dans le cadre de ce processus d'harmonisation, les deux pays devront également se pencher sur l'action des groupes de travail nationaux chargés de la lutte contre d'autres types de fraude transfrontalière et, dans les cas où cela serait utile, prendre des mesures analogues afin, là encore, d'harmoniser les stratégies.***

En 2005, les divers organismes canadiens d'application de la loi ont mis sur pied un groupe de travail national sur la stratégie de lutte contre la fraude par marketing de masse. Ce groupe de travail, qui a bénéficié des connaissances et des conseils des divers services canadiens et américains d'application de la loi, a convenu d'une stratégie à quatre volets en vue du contrôle, du démantèlement et de la neutralisation des opérations frauduleuses de télémarketing au Canada et à l'échelle internationale. Les quatre volets de cette stratégie sont : 1) une mise en application plus vigoureuse de la législation; 2) une meilleure sensibilisation du public qui devra en outre être encouragé à signaler plus systématiquement les cas de fraude dont il aurait connaissance; 3) le renforcement des sanctions et l'adoption de mesures mieux ciblées et plus précises; et 4) le renforcement de la coopération et la mise en commun des renseignements[97]. L'adoption et la mise en œuvre de cette stratégie exigera naturellement que le Canada et les États-Unis poursuivent leur étroite collaboration au niveau des moyens stratégiques et tactiques de lutte contre les divers types de fraude par marketing de masse.

2. Les efforts sur le plan opérationnel

3) ***Les organismes officiels membres des actuels groupes de travail interorganismes sur la fraude par télémarketing devront non seulement confirmer leur volonté de participer pleinement aux travaux de ces groupes de travail, mais également envisager d'y accueillir de nouveaux partenaires lorsque cela permettrait de mobiliser des ressources supplémentaires pour les enquêtes sur la fraude transfrontalière.***

Nous avons vu que, depuis la remise du rapport 2003, les moyens mis en œuvre pour combattre la fraude par marketing de masse comprennent actuellement, au Canada,

---

[97] Voir JESSE CALE, JOHN WINTERDYK, NIKKI THOMPSON & PATRICK NEAL, TOWARDS A NATIONAL STRATEGY AGAINST MASS MARKETING FRAUD IN CANADA (2007), consultable à http://www.bpcpa.ca/images/content/publications/nmmf%20strategy%20report2007.pdf.

six groupes de travail et partenariats stratégiques. Certains organismes ne participent plus aux travaux de certains de ces groupes de travail et partenariats, mais le travail effectué depuis 2003 démontre la réelle utilité de l'action de ces groupes de travail et partenariats dans la lutte contre la fraude transfrontalière par marketing de masse. Afin de poursuivre les efforts engagés, les principaux participants à ces groupes de travail et partenariats devront poursuivre leur collaboration et, le cas échéant, accueillir les représentants d'autres services d'application de la loi ou organismes réglementaires oeuvrant aux divers paliers de gouvernement afin de renforcer leurs moyens de lutte et les adapter aux évolutions des phénomènes frauduleux.

4) ***Lors de leurs enquêtes et de la préparation des poursuites engagées contre les auteurs de divers stratagèmes de fraude transfrontalière, la police, les agents des divers services d'application de la loi et les responsables des poursuites pénales devront envisager toute la gamme de mesures de saisie et de confiscation des revenus tirés de ces fraudes et en restituer le maximum aux victimes.***

Depuis 2003, les services d'application de la loi des deux pays se sont davantage attachés à retrouver, à saisir et à confisquer les produits de ces grosses combines frauduleuses faisant appel aux techniques du marketing de masse. Il n'est manifestement pas possible de récupérer dans tous les cas le produit des activités frauduleuses, mais tant les services policiers que les services des poursuites devraient garder à l'esprit, dans le cadre de leur action contre tel ou tel stratagème de fraude, les possibilités de saisir et de confisquer les produits de la criminalité et de recourir pour cela à tous les moyens que leur offre la loi.

5) ***Lors d'enquêtes sur des affaires de fraude transfrontalière, les ministères publics des deux pays devraient traiter avec célérité les demandes d'entraide judiciaire et chercher les moyens d'une encore plus grande diligence.***

Depuis le rapport de 2003, le Forum de prévention de la criminalité transfrontalière s'est penché sur la question et a délégué ce dossier au sous-groupe des poursuites pénales. Ce sous-groupe s'est, pour sa part, penché systématiquement sur la question du traitement diligent des demandes présentées au titre du traité d'entraide juridique Canada-États-Unis ou du traité d'extradition.

6) ***Les services des poursuites pénales et organismes d'exécution civile des deux pays devront en outre décider s'il ne conviendrait pas de recourir davantage aux « sweeps », c'est-à-dire à des séries d'actions répressives coordonnées lancées contre un type précis d'activité criminelle ou frauduleuse dans certains dossiers de fraude transfrontalière.***

Depuis la remise du rapport de 2003, les services d'application de la loi des deux pays ont lancé deux grandes rafles multinationales visant des catégories précises de fraude par marketing de masse. D'abord, l'Attorney General des États-Unis, de concert

avec ses homologues canadiens et les représentants d'autres services d'application de la loi, a annoncé le lancement de l'opération « Roaming Charge ». Cette opération, annoncée officiellement par l'Attorney General des États-Unis et les représentants de services canadiens et autres, le 5 octobre 2004, est la plus grande opération multinationale de ce genre jamais lancée contre des organisations de fraude par télémarketing opérant à l'échelle nationale ou internationale. Cette opération qui a pris neuf mois et exigé plus de 100 enquêtes différentes a permis de dénombrer plus de cinq millions de victimes dont les pertes s'élevaient à plus d'un milliard de dollars. Ce coup de filet a permis l'arrestation de plus de 100 personnes aux États-Unis, et de 35 autres dans divers autres pays. Cela a notamment exigé la délivrance de plus de 190 mandats de perquisition par les autorités américaines et canadiennes. Lorsque l'opération a été officiellement annoncée, 70 individus avaient déjà été condamnés, les procureurs généraux des États concernés ayant engagé, contre des opérations de télémarketing illicites, 270 actions pénales, civiles et réglementaires[98].

Plus récemment, le 23 mai 2006, l'Attorney General des États-Unis, et d'autres officiels responsables de l'application de la loi ont annoncé les résultats de l'opération « Global Con ». Cette opération, menée pendant 15 mois au cours de la période 2005-2006, était à la fois la plus vaste et la plus ambitieuse des opérations multinationales de lutte contre la fraude par marketing de masse. Les 96 enquêtes distinctes menées par les autorités américaines dans le cadre de cette opération, ont permis d'identifier plus de 2,8 millions de victimes, dont les pertes s'élevaient à plus d'un milliard de dollars. Cent trente-neuf individus ont été arrêtés aux États-Unis, 426 autres arrestations étant effectuées au Canada, au Costa Rica, aux Pays-Bas et en Espagne. Dans les cinq pays, 447 mandats de perquisition ont été exécutés. À la date où l'opération a été annoncée, 61 condamnations avaient déjà été prononcées, et 20 actions civiles intentées par la FTC contre 140 défendeurs différents[99].

Ces opérations de grande envergure telle que Roaming Charge et Global Con présentent plusieurs avantages du point de vue de la répression des fraudes. Non seulement permettent-elles de sensibiliser l'opinion publique, mais elles confirment l'importance de la planification à long terme, de la mise en commun des renseignements et de la coordination entre services policiers des divers pays. Pour lutter efficacement contre la fraude internationale, les services d'application de la loi vont devoir mettre en commun non seulement les renseignements mais également les moyens dont ils disposent afin de pouvoir déceler et contrer les auteurs des grandes fraudes par marketing de masse et, en même temps, recueillir sur la criminalité des renseignements utiles aux autorités des divers pays, non seulement pour réprimer les activités criminelles mais aussi pour

---

[98] Voir U.S. Dep't of Justice, communiqué de presse, 5 octobre 2004, consultable à http://www.usdoj.gov/opa/pr/2004/October/04_crm_680.htm.

[99] Voir U.S. Dep't of Justice, communiqué de presse, 23 mai 2006, consultable à http://www.usdoj.gov/opa/pr/2006/May/06_crm_321.html.

mieux faire comprendre à leurs populations les risques auxquels elles sont exposées. Les organismes, qui, dans les deux pays, sont chargés des enquêtes ou des poursuites pénales devraient envisager, selon les circonstances, de lancer d'autres opérations de grande envergure contre les réseaux de fraude par marketing de masse, d'obtenir la participation d'autres pays et de parvenir ainsi à une démultiplication des efforts engagés.

7) ***Dans les deux pays, les services d'application de la loi et les responsables des poursuites pénales devront se pencher sur la manière d'utiliser plus efficacement, les moyens de vidéoconférence pour recueillir la déposition de témoins habitant les États-Unis.***

Depuis le rapport 2003, les deux pays reconnaissent que les vidéoconférences continuent à présenter les mêmes avantages et inconvénients qu'avant (en l'occurrence les complications logistiques et les coûts) lorsqu'il s'agit de produire certains témoignages dans le cadre d'actions engagées au Canada. Les organismes américains devraient donc être disposés à répondre en ce domaine aux demandes formulées par les autorités canadiennes lorsqu'il convient de recueillir, à distance, la déposition d'un résident de États-Unis, et à s'entendre sur le partage des frais et des efforts que cela implique.

3. La mise en commun des renseignements

8) ***Les deux pays devront prendre des mesures afin de diffuser plus rapidement, tant au niveau national qu'entre groupes de travail interorganismes, actuels ou à venir, les informations publiques concernant les mesures prises par les services policiers, les responsables des poursuites publiques et les autorités réglementaires afin de réprimer les fraudes transfrontalières dans l'un et l'autre pays, y compris les renseignements concernant les risques que ces divers types de fraude posent aux individus et aux entreprises.***

Les efforts engagés en ce sens depuis le rapport de 2003 demeurent insuffisants. Certes, le Canada et les États-Unis sont, chacun de leur côté, parvenus à mieux faire connaître au public les mesures prises afin de lutter contre la fraude par marketing de masse, mais les deux pays doivent adopter en ce domaine des approches plus systématiques et mettre en place des mécanismes permettant de diffuser ces renseignements plus rapidement à leurs services respectifs ainsi qu'aux autorités d'autres pays. Nos deux pays ont déjà commencé à mettre en place de tels mécanismes et se sont déjà entendus sur des pratiques qui s'annoncent prometteuses.

9) ***Nos deux pays devront coordonner leurs efforts au niveau des contacts avec d'autres pays dont les citoyens sont impliqués dans des combines frauduleuses transfrontalières, et mettre davantage en commun avec les services officiels de ces pays, les renseignements et les moyens de formation adaptés au problème. Ils devront en outre prendre les mesures nécessaires pour améliorer la coopération et la***

coordination avec ces divers pays au niveau des enquêtes et de la répression de fraudes.

Les deux pays ont, depuis le rapport 2003, pris plusieurs mesures afin de mieux coordonner leur action avec des pays tels que l'Australie, la Nouvelle-Zélande et le Royaume-Uni. Comme nous l'avons vu, les fraudes transfrontalières touchent de plus en plus de pays. Les services policiers de nos deux pays pourraient ainsi s'échanger les renseignements concernant leurs contacts dans d'autres pays les mieux à même de faciliter la coordination des mesures de lutte contre la fraude transfrontalières, de faciliter l'échange d'informations sur les fraudes et d'examiner ensemble les divers moyens de mieux combiner les renseignements et les moyens de formation.

4. La coordination entre les secteurs publics et privés

10) ***Les deux pays devraient coordonner aussi leurs efforts de concertation avec le secteur des services financiers et des modes de paiement électronique afin de s'entendre sur les moyens de réduire le recours à certains mécanismes de paiement actuellement employés par les auteurs de fraudes transfrontalières***

Depuis le rapport remis en 2003, dans les deux pays, divers organismes ont entrepris de se concerter avec des établissements financiers au sujet des abus auxquels peuvent donner lieu certains moyens de paiement tels que les transferts monétaires et les transferts électroniques de fonds. Les deux pays n'ont cependant pas encore appliqué la recommandation concernant la coordination des efforts binationaux dans le cadre de telles concertations. Les gouvernements des deux pays auraient tout intérêt à coordonner leurs efforts en ce domaine, notamment en ce qui concerne le recours abusif à certains mécanismes de paiement tels que les transferts de fonds, les entreprises de traitement des paiements, et l'emploi de plus en plus fréquent de faux chèques par les auteurs de fraudes par marketing de masse.

5. La formation

11) ***Les deux pays devraient organiser au moins une fois par an une conférence au cours de laquelle les enquêteurs et les responsables des poursuites pénales peuvent procéder à un échange de renseignements au sujet des nouvelles tendances et de la tournure des activités frauduleuses transfrontalières, et recevoir un complément de formation afin de parfaire leur connaissance des techniques d'enquête et de règles de droit et de procédure qui ont fait leurs preuves dans le cadre de la lutte contre les fraudeurs de grande envergure.***

Depuis le rapport 2003, les deux pays ont continué à organiser des conférences annuelles afin d'étudier ensemble les nouvelles tendances et évolutions des fraudes transfrontalières et assurer un complément de formation en matière de droit et de techniques d'enquête adaptées à ce genre de criminalité. Tout récemment, en févier 2008,

le Alberta Partnership Against Cross Border Fraud, partenariat regroupant, au Canada, le Groupe de travail sur la stratégie nationale de prévention de la fraude par marketing de masse et le Centre d'appel antifraude du Canada (PhoneBusters) a organisé à Banff (Alberta), un atelier de formation à l'intention des enquêteurs internationaux. Cet atelier, au cours duquel ont pris la parole des représentants de nombreux services d'application de la loi canadiens, américains et autres, a réuni plus de 200 participants. En outre, le National Advocacy Center, rattaché au département américain de la Justice assure, plus ou moins tous les ans, trois séminaires de formation sur la criminalité internationale en col blanc, auxquels sont conviés des représentants des services d'application de la loi d'autres pays. Les participants à ces conférences et séminaires reconnaissant tous l'utilité de ces rencontres, tant pour les enquêteurs que pour les procureurs, et nos deux pays devraient continuer à se réunir chaque année pour examiner, ensemble, les moyens de rendre toujours plus efficace le partage des renseignements sur l'évolution des techniques de fraude par marketing de masse, et mettre en commun certains moyens de formation.

12) ***Les deux pays devraient se concerter sur l'emploi des vidéoconférences comme moyen de formation binationale ou multinationale sur divers aspects de la fraude à grande échelle.***

Nos deux pays, comme l'indique le rapport de 2003, ont eu recours aux vidéoconférences comme moyen de formation. Les États-Unis et le Canada conviennent de continuer.

B. Recommandation d'ordre général

13) Que les deux pays consolident leurs activités de renseignement policier sur la progression du phénomène de la fraude par marketing de masse et, dans le respect des règles de droit applicables, mettant ces renseignements en commun et en fassent bénéficier les services de police de divers autres pays.

Dès qu'ils relèvent un nouveau cas de fraude internationale par marketing de masse – tel que la progression et le développement de groupements criminels liés au Nigeria, qui se livrent à un étonnant éventail d'escroqueries au moyen des techniques du marketing de masse, les services policiers des deux pays doivent très rapidement s'entendre sur les types de renseignements qu'il leur faut acquérir en priorité pour suivre l'évolution de la criminalité, et sur les meilleurs moyens de les recueillir, de les analyser et de les diffuser sous une forme utile à d'autres services d'application de la loi ou organismes régulateurs. Les deux pays doivent l'un et l'autre agir dans le respect des normes juridiques qui gouvernent la collecte et le partage des renseignements, mais les services intéressés doivent agir plus efficacement pour contrer les principaux types d'escroqueries par marketing de masse et les nouveaux types de fraude qui se manifestent. L'expérience acquise dans ce domaine, tant au niveau des enquêtes que des poursuites engagées, démontre que pour combattre la fraude par marketing de masse, la

collaboration simplement binationale ne suffit pas et c'est désormais la coopération multinationale qui s'impose.

* * *

Au cours de ces dix premières années de coopération binationale officielle, le Canada et les États-Unis ont resserré leurs liens en matière de partage des renseignements, d'action répressive, d'information et de sensibilisation du public, de prévention et d'actions en justice afin d'accroître l'efficacité de leur lutte contre les diverses fraudes par marketing de masse. Il s'agit maintenant, d'entretenir et de consolider cette base pour faire face à la menace polyvalente que crée la fraude par marketing de masse, qui pose des risques non seulement pour les consommateurs et les établissements commerciaux mais, aussi, pour les gouvernements.