Mass-Marketing Fraud

A Report to the Minister of Public Safety of Canada
and the Attorney General of the United States

March 2008

***

Mass-Marketing Fraud Subgroup
Cross Border Crime Forum

Table of Contents

* * *

Introduction

In April 1997, then-Prime Minister of Canada Jean Chrétien and then-President of the United States Bill Clinton directed the preparation of a joint study examining ways to counter the serious and growing problem of cross-border telemarketing fraud. In November 2007, a binational working group established for that purpose provided a report to the Prime Minister and the President that contains a detailed examination of the problem and a series of recommendations to improve both countries' responses to the problem.[1] Those recommendations included identification of telemarketing fraud as a serious crime; establishment of regional task forces to cooperate across the international border; coordination of strategies to control telemarketing fraud between both countries at agency, regional, and national levels; operation of an ongoing binational working group to provide overall coordination; and other recommendations to address information-gathering, evidence-sharing and mutual legal assistance, extradition, and public education and prevention.[2]

The 1997 Report became a general blueprint for coordinated binational actions against telemarketing fraud. In the ten years since the issuance of the 1997 Report, Canada and the United States have not only carried out all of the recommendations in that Report, but have made even greater strides in combating what is now termed mass-marketing fraud - i.e., fraud schemes that use mass communications methods, such as telemarketing, the Internet, and mass mailing to contact and communicate with large numbers of prospective victims and to obtain funds from victims.

This Report has three purposes. First, it will describe the principal trends and developments since 2003 in four major types of crime associated with mass-marketing fraud (i.e., telemarketing fraud schemes, Internet fraud schemes, Nigerian fraud[3], and identity theft). Second, it will summarize the principal approaches that law enforcement in both countries have adopted since 2003 to combat mass-marketing fraud more effectively. Third, it will report on recommendations that this Subgroup made in 2003 as part of a binational action plan to combat mass-marketing fraud, and set out additional recommendations that address changes in the nature and types of mass-marketing fraud that have emerged since 2003.

---

[1] *See* UNITED STATES - CANADA WORKING GROUP, UNITED STATES - CANADA COOPERATION AGAINST CROSS-BORDER TELEMARKETING FRAUD (November 1997) (hereinafter 1997 Report), *copy available at* http://strategis.ic.gc.ca/pics/ct/reporte.pdf.

[2] *See, e.g., id.* at 7, 20-22, 25, 28, 29.

[3] Canadian authorities refer to "West African Fraud".

Section I: Mass-Marketing Fraud in Canada and the United States

For more than a decade, Canada and the United States have been actively combating the problem of mass-marketing fraud. Although it originally encompassed only cross-border telemarketing fraud, mass-marketing fraud affecting both countries has since expanded into a multifaceted problem that includes traditional telemarketing fraud, Internet fraud, Nigerian fraud, and identity theft. The 2006 joint Canada/United States Organized Crime Threat Assessment observed that identity theft, Internet fraud, and money laundering were among the financial crimes "that are growing in scale, scope, and sophistication."[4] Moreover, newer developments – including the dramatically increased use of counterfeit checks and money orders, and the substantial use of various payment mechanisms such as payment processors and money transfer businesses in connection with mass-marketing fraud schemes – have further complicated the tasks of law enforcement in mounting effective responses to cross-border mass-marketing fraud.

This Section of the report will discuss the principal trends and developments since 2003 in cross-border telemarketing fraud, Internet fraud, Nigerian fraud, and identity theft.

A. Telemarketing Fraud

1. Background

Telemarketing fraud is both the oldest and, in some respects, the most persistent form of mass-marketing fraud that Canada and the United States must combat. As the 2006 Canada/United States Organized Crime Threat Assessment noted, telemarketing fraud "continues to target both Canadian and US citizens."[5]

In the United States, a private non-profit entity, the National Consumers League (NCL) reported that in 2006 (the most recent year for which data are available) the ten leading types of telemarketing fraud were as listed below in Table I:[6]

---

[4] 2006 CANADA/US ORGANIZED CRIME THREAT ASSESSMENT, *available at* http://www.rcmp-grc.gc.ca/organizedcrime/octa_e.htm.

[5] *Id.*

[6] *See* National Consumers League, 2006 Top 10 Telemarketing Scam Trends from NCL's Fraud Center, January – December 2006 [hereinafter NCL 2006 TELEMARKETING TRENDS], *available at* http://fraud.org/stats/2006/telemarketing.pdf.

TABLE I: NATIONAL CONSUMERS LEAGUE FRAUD CENTER, 2006 TELEMARKETING FRAUD DATA		
Type of Scheme	***Percentage of Complaints***	***Average Victim Loss***
1. Fake Check Schemes	31	$3,278
2. Prize/Sweepstakes Schemes	26	$2,749
3. Magazine Sales	8	$77
4. Scholarships/Grants	6	$236
5. Advance Fee Loans	6	$1,164
6. Lotteries/Lottery Clubs	6	$3,189
7. Credit Card Offers	4	$237
8. Phishing	3	$387
9. Work-at-Home Plans	1	$104
10. Travel/Vacation	1	$812

Two observations about these data are in order. First, fake check schemes – in which victims are persuaded to deposit checks that later prove to be counterfeit into their bank accounts and to send the criminals a portion of the deposited check – not only were the leading type of complaint but also generated the highest average loss per victim. Second, lotteries and lottery clubs accounted for the second highest average loss, but constituted only 6 percent of the complaints, while prize and sweepstakes schemes were the second leading type of telemarketing scheme and generated the third highest average loss.

With respect to these 2006 data, the NCL reported that the five leading locations of telemarketing fraud schemes that U.S. consumers reported were as follows: (1) Canada (30 percent); (2) Countries outside the United States and Canada (15 percent); (3) Florida (8 percent); (4) New York (7 percent); and (5) California (5 percent). The NCL also noted that foreign telemarketing fraud schemes targeting U.S. residents accounted for 45 percent of all complaints in 2006 – a substantial increase from 2006 (26 percent).[7]

In Canada, PhoneBusters, the Canadian Anti-fraud Call Center, reported the following data for various fraudulent solicitations from 2005 to 2007:[8]

[7] *See id.*

[8] *See* Phonebusters, Monthly Summary Report (2007), *available at* http://www.phonebusters.com/english/documents/Yearly2007_000.pdf.

Table II: Phonebusters 2005-2007 Fraud Complaint Data (Including Prize, Loan, Vacation and Other Schemes)			
	2005	***2006***	***2007***
Canadian Attempts	11,306	10,830	14,433
Canadian Victims	4,608	4,192	4,124
Value of Canadian Loss Reported	$16,498,990.70	$24,532,680.04	$18,177,921.36
U.S. Attempts	10,668	13,350	9,069
U.S. Victims	12,214	10,908	8,684
Value of U.S. Loss Reported	$58,432,710.73	$48,830,098.19	$35,438,164.96
U.K. Attempts	32	16	14
U.K. Victims	115	47	56
Value of U.K. Loss Reported	$730,925.99	$1,296,538.41	$987,924.05
Other Countries/Unknown Attempts	186	76	72
Other Countries/Unknown Victims	169	87	177
Value of Other Countries/Unknown Losses Reported	$657,909.58	$1,383,452.12	$4,099,652.54
Total Fraud Attempts	22,192	24,272	23,588
Total Fraud Victims	17,106	15,234	13,041
Total Fraud Loss Reported	$76,320,537.00	$76,042,768.76	$58,703,662.91

Several observations about these data are in order. First, while the number of attempted fraud contacts with Canadian residents increased from 2006 to 2007, the number of actual Canadian victims remained virtually the same but the total amount of Canadian loss declined by one-third. Second, the numbers of U.S. attempted fraud contacts with U.S. residents and actual U.S. victims, as well as the total amount of U.S. loss, (as reported to PhoneBusters) all declined from 2006 to 2007. Third, the small number of attempted fraud contacts with U.K. residents and the total amount of U.K. loss declined slightly from 2006 to 2007. Fourth, the number of victims from other countries (or unknown locations), and the total amount of their loss, substantially

increased from 2006 to 2007, as the number of victims more than doubled and the total loss nearly tripled.

2. Trends

In general, some features of cross-border telemarketing fraud, such as substantial reliance on money transfer businesses to receive proceeds from victims, have remained in use over the past several years. Other characteristics, however, have undergone substantial transformation since 2003, as described below:

a. Involvement of Organized Crime

The most far-reaching change in cross-border telemarketing fraud since 2003 is the substantial and growing involvement of Nigerian-led criminal rings in telemarketing fraud and other financial fraud, including Internet fraud schemes such as "phishing"[9] and various schemes that involve use of counterfeit checks.[10] Law enforcement authorities report that while they believe certain elements of traditional hierarchical organized crime groups continue to be involved in cross-border telemarketing fraud – particularly with respect to the provision of "leads" (i.e., names and related data of prior fraud victims), "protection"[11] of telemarketing-fraud rooms, and money laundering services – the number of Nigerian-led fraud operations has increased significantly in several major metropolitan areas of Canada, as they have in several West African countries and various European countries such as the Netherlands, Spain, and the United Kingdom. These Nigerian-led rings routinely use the services of multiple individuals in often elaborate and carefully conducted schemes, often performing specific functions in multiple countries, though they lack the hierarchical characteristics of various ethnic organized criminal groups in North America and Europe.

b. "Pitches" and Other Operational Features

For non-Nigerian criminal operations, many of the telemarketing fraud "pitches" (i.e., false or fraudulent stories and explanations for the criminals' requests or demands for payments by prospective victims) that were prevalent in the first part of this decade have continued to be extensively used in the last five years. These include fraudulent offers of prizes or sweepstakes or lottery winnings, fraudulent offers of "guaranteed" credit cards or loans, and so-called "business-to-business" schemes (i.e., offers of listings in nonexistent business directories, or of

---

[9] *See* p. 12 *infra*.

[10] *See* 2006 CANADA/US ORGANIZED CRIME THREAT ASSESSMENT, *supra* note 3.

[11] Other organized crime groups extort payments from telemarketing fraud operators.

office-related supplies and products).[12] These schemes can be extraordinarily lucrative. For example, the co-owner of two telemarketing firms that operated in Montreal and Toronto and targeted exclusively U.S. companies with fraudulent business directory listings and other schemes was recently convicted at trial of violating ten counts of the Competition Act by making false or misleading representations through his firms. According to one estimate, the two firms were estimated to have had more than $70 million in sales.[13]

With the growing incursion of Nigerian-led fraud schemes based in Canada, law enforcement authorities have seen movement toward a wider variety of advance-fee schemes that are characteristic of Nigerian criminal rings. These include fraudulent solicitations that seek to persuade a prospective victim to deposit into the victim's personal bank account a check sent by the scheme to and wire-transfer a portion of the funds back to the control of the scheme. Victims routinely do so, only to find out at a later date that the checks are counterfeit and that they not only have lost the funds wired to the scheme but are liable to the bank where the check was deposited for the full face amount of the check.

Law enforcement authorities have noted that certain schemes operated by Nigerian criminal rings often use regular mail and email as the initial method of contacting victims, but then rely extensively on telephonic contact with a victim who had responded positively to the initial mail solicitation. As indicated above, some Nigerian-related schemes engage in identity theft through online techniques such as "phishing" to acquire victims' personal identifying and financial account data.

c. Concealment Techniques

---

[12] Within Canada, cross-border business-to-business schemes appear to be especially prevalent in the Montreal area. Law enforcement authorities estimate that there are approximately 50 known business-to-business operations in Montreal, each typically employing between 10 and 30 people. Some business-to-business operations, however, have been substantially larger. In October 2007, law enforcement authorities in Montreal raided one large "business-to-business" operation that occupied several floors of a single office building and employed approximately 100 "pitchers" (i.e., employees who called prospective victims) to "pitch" business directories and first-aid kits. The operation reportedly targeted small and medium-sized busineses in Canada, the United States, and Europe. That raid resulted in more than 120 arrests. *See* Jan Ravensbergen, *Alleged fraud ring busted*, Montreal Gazette, October 9, 2007, *available at* http://www.canada.com.

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

One technique that law enforcement authorities report cross-border fraud schemes are increasingly using is the Voice over Internet Protocol (VoIP) technology. VoIP has been defined as

> a technology that allows you to make voice calls using a broadband Internet connection instead of a regular (or analog) phone line. Some VoIP services may only allow you to call other people using the same service, but others may allow you to call anyone who has a telephone number - including local, long distance, mobile, and international numbers. Also, while some VoIP services only work over your computer or a special VoIP phone, other services allow you to use a traditional phone connected to a VoIP adapter.[14]

Because VoIP services can allow the VoIP user to display to callers a telephone number different from the actual number at which the VoIP user is located, fraud schemes can mislead prospective victims into thinking that the location they are calling is in a different location (e.g., a Florida-based investment fraud scheme that falsely displays a telephone number in the 212 (New York City) area code, or a Toronto-based advance-fee scheme that falsely displays a telephone number in a non-Toronto area code). Law enforcement authorities have noticed the use of VoIP technology by major telemarketing fraud operations in Canada and Costa Rica that targeted U.S. victims.

d. Methods of Transmitting Funds

In general, the period from 2003 to 2008 saw a continuation of the trend towards having victims transmit their payments to fraud schemes by wire transfer, particularly the leading money-transfer businesses Western Union and MoneyGram. For example, in the United States, the National Consumers League reported that in 2006 wire transfer was by far the leading mode of payment in telemarketing schemes, accounting for 54 percent of all complaints that reported a mode of payment. The next three types of payment accounted for another 35 percent of complaints: (2) bank debits (14 percent); (3) checks (11 percent); and credit cards (10 percent).[15]

In the first several years of this decade, law enforcement authorities, particularly in Québec, noted that organized criminal group members in some cases had sought either to compromise or to threaten agents with money transfer services, to reduce the amount of record-keeping associated with receipt of funds transfers from fraud victims. Law enforcement authorities are now seeing that in some areas of Canada, members of Nigerian criminal rings, in order to avoid detection, are applying for and receiving Money Gram and Western Union

---

[14] Federal Communications Comm'n, IP-Enabled Services, *available at* http://www.fcc.gov/voip/.

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

franchises. These franchises are operated only as store fronts and are solely used for money laundering purposes rather than legitimate business activity.

B. Internet Fraud

1. Background

Since the creation of the World Wide Web, law enforcement authorities in North America have observed a wide variety of fraud schemes that use the Internet for various purposes, ranging from initial contact with prospective victims to receiving and laundering funds from victims. The most current U.S. statistical data regarding complaints about Internet fraud are available in a February 2008 report by the Federal Trade Commission (FTC). These data reflect Internet fraud-related complaints that the FTC received from 2005 through 2007, as shown below in Table III:[16]

Table III: FTC 2005-2007 Internet Fraud-Related Complaint Data			
	2005	***2006***	***2007***
Number of Complaints	197,085	205,269	221,226
Total Amounts of Loss Reported	$336,345,604	$590,494,777	$525,743,643
Average Amount Paid	$2,095	$3,332	$2,730
Median Amount Paid[17]	$342	$500	$395

Several aspects of these data deserve mention. While the total number of Internet-related fraud complaints in 2007 increased by nearly 8 percent since 2006, the total loss, average, and median amounts all decreased from 2006. At the same time, total losses reported in 2007 still exceed $525 million, an exceptional amount of reported financial loss for any type of fraud. In addition, because the average amount paid by victims of Internet-related fraud schemes (i.e., the total amount paid divided by the number of victims who reported the amounts paid) substantially exceeds the median amount paid in all three years, it appears that a number of large payments by victims is skewing the average amount paid in each of the three years. For example, in 2007, the complaint data indicate that 83 percent of those complaints who reported loss amounts reported

[16] *See* FEDERAL TRADE COMM'N, CONSUMER FRAUD AND IDENTITY THEFT COMPLAINT DATA: JANUARY-DECEMBER 2007 at (February 2008) [hereinafter FTC 2007 COMPLAINT DATA], *available at* http://www.ftc.gov/opa/2008/02/fraud.pdf.

[17] The FTC stated that "Median is the middle number in a set of numbers so that half the numbers have values that are greater than the median and half have values that are less. Calculation of the median excludes complaints with amount paid reported as $0." *Id.* at 10.

amounts of $1,000 or less, while 12 percent (22,458) reported payments of $1,000 to $5,000 and another 4 percent (7,017) reported payments of more than $5,000.[18]

2. Trends

In the United States, the FTC reported the following data showing changes with respect to methods of payments during the period 2005-2007, as shown below in Table IV:[19]

Table IV: Methods of Payment Reported by Consumers to FTC For Internet-Related Fraud Complaints, 2005-2007 [Amounts (Number of Complaints)]

	2005	***2006***	***2007***
Bank Account Debit	$11,181,001 (6,153)	$21,792,498 (6,643)	$13,751,585 (6,653)
Cash/Cash Advance	$11,164,636 (1,039)	$7,648,293 (1,169)	$7,943,260 (1,216)
Check	$21,804,907 (3,437)	$60,119,725 (2,850)	$17,906,180 (2,577)
Credit Cards	$19,004,962 (12,208)	$24,736,839 (12,927)	$30,681,611 (14,822)
Money Order	$7 ,839,943 (3,997)	$16,661,396 (3,660)	$25,663,620 (2,962)
Telephone Bill	$96,364 (424)	$259,659 (429)	$112,452 (298)
Wire Transfer	$41,786,350 (5,557)	$91,623,738 (8,769)	$76,670,821 (10,857)

These data are noteworthy in several respects. First, payments by wire transfer continue to be the highest-dollar total of payments, even though the total amount of 2007 wire transfer payments declined from 2006 even as the number of complaints reporting such transfers increased by nearly 24 percent since 2006. Second, credit cards remained a distant second to wire transfer as a method of payment, but the amount of credit-card payments increased by 24 percent over 2006 and the average credit-card payment in 2007 ($2,070) increased by more than 8 percent over the average credit-card payment in2006. Third, from 2006 to 2007 there was substantial declines in both the total amounts of reported payments by checks ($60 million to nearly $18 million) and bank account debits (nearly $22 million to nearly $14 million), even though the number of complaints reporting such payments did not change significantly from one year to the next. Fourth, there was a substantial increase from 2006 to 2007 in the amounts of payments by money orders (more than $16 million to more than $25 million), even as the number of complainants reporting such payments decreased by nearly 24 percent.

[18] *Id.*

[19] *See id*. at 11.

Additional trend data are available from the Internet Crime Complaint Center (IC3), a partnership of the FBI and the National White Collar Crime Center. The IC3 reported the following data for complaints it received in 2006:

> The total dollar loss from all referred cases of fraud was $198.44 million with a median dollar loss of $724.00 per complaint. This is up from $183.12 million in total reported losses in 2005. Other significant findings related to an analysis of referrals include:
>
> - Internet auction fraud was by far the most reported offense, comprising 44.9% of referred complaints. Non-delivered merchandise and/or payment accounted for 19.0% of complaints. Check fraud made up 4.9% of complaints. Credit/debit card fraud, computer fraud, confidence fraud, and financial institutions fraud round out the top seven categories of complaints referred to law enforcement during the year.
>
> - Of those individuals who reported a dollar loss, the highest median losses were found among Nigerian letter fraud ($5,100), check fraud ($3,744), and other investment fraud ($2,695) complainants.
>
> - Among perpetrators, 75.2% were male and half resided in one of the following states: California, New York, Florida, Texas, Illinois, Pennsylvania and Tennessee. The majority of reported perpetrators were from the United States. However, a significant number of perpetrators where also located in United Kingdom, Nigeria, Canada, Romania, and Italy.
>
> - Among complainants, 61.2% were male, nearly half were between the ages of 30 and 50 and one-third resided in one of the four most populated states: California, Texas, Florida, and New York. While most were from the United States, IC3 received a number of complaints from Canada, Great Britain, Australia, India, and Germany.
>
> . . .
>
> - Recent high activity scams seen by IC3 include hit man scams, phishing attempts associated with spoofed sites, and counterfeit checking scams.[20]

[20] INTERNET CRIME COMPLAINT CENTER, INTERNET CRIME REPORT: JANUARY 1, 2006 - DECEMBER 31, 2006 at 3 (2007), *available at* http://www.ic3.gov/media/annualreport/2006_IC3Report.pdf.

In addition, the National Consumers League (NCL), reported that the top ten Internet fraud schemes reported to it in 2006 were as shown in Table V below.[21] Several aspects of these data are noteworthy. First, online investment schemes appear to have surged in 2006. Those schemes not only generated the highest average loss of the top ten Internet schemes in 2006, but were in the top ten for the first time in a decade.[22] Second, fake check scams generated the second-highest average loss, even though they represented only 11 percent of complaints to the NCL. Because many fake check schemes are conducted by West African criminal rings, it is possible that some of the rings conducting those schemes are also involved in the Nigerian money offers that generated other complaints.

Table V: NCL 2006 Internet Fraud Complaint Data

	Percentage of All Complaints	*Average Loss*
1. Auctions	34	$1,331
2. General Merchandise	33	$1,197
3. Fake Check Scams	11	$4,053
4. Nigerian Money Offers	7	$3,741
5. Lotteries/Lottery Clubs	4	$1,750
6. Advance Fee Loans	3	$1,515
7. Phishing	2	No losses reported
8. Prizes/Sweepstakes	1	$2,447
9. Internet Access Services	1	$920
10. Investments	1	$4,759

Third, as with the telemarketing complaints to the NCL, wire transfers represented by far the largest single method of payment (45 percent) in the online fraud schemes reported to the NCL. Other methods of payment reported for these online fraud schemes included credit cards (20 percent); bank debit (9 percent); debit card (8 percent); money order (8 percent); check (5 percent); cashier's checks (2 percent); and cash (2 percent).[23] Finally, the five most frequent location of online fraud schemes reported to the NCL were (1) countries outside the United

[21] *See* National Consumers League, 2006 Top 10 Internet Scam Trends from NCL's Fraud Center, January – December 2006, *available at* http://fraud.org/stats/2006/internet.pdf.

[22] *Id.*

[23] *See id.*

States and Canada (38 percent); (2) California (10 percent); (3) Florida and New York (6 percent - tie); (5) Texas and Canada (4 percent - tie); and (7) Illinois (3 percent).[24]

C. Nigerian Fraud

A third significant type of mass-marketing fraud that the 2003 Report identified was Nigerian fraud: i.e., schemes, typically conducted by loosely-knit criminal networks with Nigerian affiliations, that involve various types of fraudulent solicitations by mail, fax, telephone, and email. These solicitations include, for example, offers of bogus opportunities to assist African residents in laundering illegal proceeds or transferring other funds out of Africa. There is a consensus among North American, European, and Nigerian law enforcement experts on Nigerian fraud schemes that these schemes, regardless of the type of fraud scheme or location of their principal operations, are conducted by loose-knit criminal networks dominated by individuals with Nigerian nationality or Nigerian tribal or family relationships, though lower-level participants in the scheme may include individuals with other West African nationalities as well as non-African nationalities.

In the United States, while there are no aggregate statistical data on the number of U.S. residents who are contacted in some manner by these schemes, the FTC's 2008 Consumer Fraud and Identity Theft Complaint Data shows that "Foreign Money Offers" is the fourth largest complaint category, with 32,868 complaints in Consumer Sentinel (or 4% of complaint total). In Canada, PhoneBusters has compiled the following data for Nigerian letter fraud schemes during the period 2005 to 2007, as shown in Table VI:[25]

Table VI: PhoneBusters 2005-2007 Nigerian Letter Scam Complaint Data

	2005	***2006***	***2007***
Canadian Victims	175	192	152
Total Amount of Loss Reported	$9,168,422.34	$3,056,355.18	$5,264,488.15

A few observations about these data are appropriate. The average reported loss in 2007 is nearly $35,000. This average loss is substantially higher than the 2006 average loss of nearly $16,000, even though the number of reporting Canadian victims in 2007 is substantially below the number of reporting victims in 2006. It is entirely possible that one or two of the reporting victims reported losses as high as hundreds of thousands or even more than one million dollars, and that one or two such reports could significantly skew the average loss upwards. At the same time, law enforcement authorities have observed that some victims of Nigerian fraud initially

[24] *See id.*

[25] *See* PhoneBusters, Monthly Summary Report, *supra* note 8.

underreport their fraud losses, in part because they find it difficult to admit to the true magnitude of their losses even after deciding to report the fact of the fraud and the loss.

Establishing the true magnitude of losses in any particular Africa-related fraud scheme is therefore particularly difficult without substantial investigation. Nonetheless, law enforcement authorities in both countries have identified the growth of these Nigerian-led fraud operations are becoming a more substantial threat to consumers in both Canada and the United States.

D. Identity Theft

1. Background

In the past five years, identity theft has become a form of crime that reaches into every corner of North America, and that affects individuals in every demographic segment as well as legitimate companies and financial institutions. Although law enforcement agencies typically regard identity theft as a crime distinct from mass-marketing fraud, some identity theft schemes rely on fraudulent and deceptive representations by criminals to deceive people into disclosing their personal and financial details.

In Canada, PhoneBusters reported the following data for Canadian identity theft for 2005 through 2007, as shown in Table VII:[26]

Table VII: PhoneBusters 2005-2007 Identity Theft Complaint Data

	2005	***2006***	***2007***
Canadians At Risk	731	730	311
Canadian Victims	12,859	13,221	4,633
Value of Loss Reported	$8,683,603.54	$15,734,254.69	$6,383,477.37

It is worth noting that according to identity theft complaints to PhoneBusters, both the numbers of Canadian victims and the total amount of Canadian loss attributable to identity theft sharply declined from 2006 to 2007.

[26] *See id.*

In the United States, the FTC reported that in 2007, identity theft, as has been the case for several years, was the most frequently reported type of consumer fraud. Identity theft accounted for 255,627 complaints in 2005, 246,124 in 2006, and 258,427 in 2007.[27]

2. Trends and Developments in Identity Theft

At present, law enforcement agencies in both countries do not have comprehensive statistical data that would allow them to track all identity theft trends with precision. Available statistical and other data, however, have enabled law enforcement agencies in Canada and the United States to identify certain significant trends over the past five years.

a. Identity Theft Techniques

(1) *Phishing*

One significant identity theft technique for which there are substantial long-term statistical data is "phishing." Phishing is a generic term used to refer to criminals' creation and use of emails and websites designed to look like those of legitimate companies and financial institutions, as a means of persuading individuals to disclose valuable personal and financial data. The 2006 Canada/United States Organized Crime Threat Assessment described phishing scams as "one of the most significant and lucrative identity theft-related threats to Internet users."[28]

Statistical data from the Anti-Phishing Working Group (APWG), a industry association focused on eliminating identity theft and fraud stemming from phishing and email "spoofing,"indicate that there are four distinct trends in phishing since 2003:

- **Incidence and Prevalence of Phishing**. Phishing may be the form of identity theft affecting North America that has grown the most dramatically in the last five years. In January 2004, the APWG published its first report on the nascent problem of phishing. The APWG reported that during that month, 176 unique phishing attacks were reported. At the time, that number of phishing attacks was believed to be significant because it represented a 52 percent increase over the number reported in December 2003.[29]

---

[27] *See* FEDERAL TRADE COMM'N, CONSUMER FRAUD AND IDENTITY THEFT COMPLAINT DATA: JANUARY - DECEMBER 2007 at 4 (February 2008).

[28] 2006 CANADA/US ORGANIZED CRIME THREAT ASSESSMENT, *supra* note 4.

[29] *See* ANTI-PHISHING WORKING GROUP, PHISHING ATTACK TRENDS REPORT: JANUARY, 2004 at 1, 3 (2004) [hereinafter APWG JANUARY 2004 TRENDS REPORT], *available at* http://www.antiphishing.org/reports/APWG.Phishing.Attack.Report.Jan2004.pdf.

Since then, the incidence and prevalence of phishing have grown vastly beyond what anyone in the public or private sector could have foreseen. In November 2007, the APWG received 28,074 unique phishing reports and found 23,630 unique phishing sites being hosted worldwide.[30] Moreover, phishing websites are being hosted in numerous countries, including the United States and various nations in Asia and Europe. In November 2007, the APWG reported that the top ten countries hosting phishing sites were: (1) China (24.21 percent); (2) United States (23.85 percent); (3) India (9.39 percent); (4) Russian Federation (8.06 percent); (5) Thailand (4.64 percent); (6) Romania (3.53 percent); (7) Germany (3.41 percent); (8) Republic of Korea (2.42 percent); (9) United Kingdom (1.47 percent); and (1) France (1.47 percent).[31]

- **Targeting of Industry Sectors**. Over time, the focus of phishing operations has consistently been on the financial services industry, but has now become almost exclusively on that industry. In January 2004, the APWG reported that 40 percent of phishing attacks involved the "hijacking" (misuse) of corporate brands in the financial sector, although certain major e-commerce companies such as eBay initially were the targets of a comparatively substantial number of phishing attacks.[32] By contrast, in November 2004, the APWG reported that in that single month, 178 distinct corporate brands had been "hijacked" in phishing attacks – the largest number of "hijacked" brands that it had ever recorded in a single month – and that 93.8 percent of all phishing attacks that month were directed at the financial services sector.[33] The APWG also reported that in November 2007, it noted "a substantial uptick in the number of Middle East and European financial services companies being targeted, . . . in addition to large US-based banking institutions and credit unions."[34]

- **Targeting of Specific Individuals**. One trend that law enforcement and information security analysts observed over the past five years has been the increased use of phishing attacks targeted at specific groups of individuals. This technique, sometimes called "spear-phishing," is intended to increase the percentage of individuals to whose data the criminals can gain access.

---

[30] *See* ANTI-PHISHING WORKING GROUP, PHISHING ACTIVITY TRENDS: REPORT FOR THE MONTH OF NOVEMBER, 2007 at 1 (2008) [hereinafter APWG NOVEMBER 2007 TRENDS REPORT], *available at* http://www.antiphishing.org/reports/apwg_report_nov_2007.pdf.

[31] *See id*. at 6.

[32] *See* APWG JANUARY 2004 TRENDS REPORT a, *supra* note 29, at 1.

[33] *See* APWG NOVEMBER 2007 TRENDS REPORT, *supra* note 30, at 1, 5.

[34] *See id.* at 5.

Recently, the APWG reported that the number of unique phishing reports in November 2007 actually represented a decrease of more than 10,600 from the preceding month. Analysts attributed this decrease, in part, to "eCrime gangs' increasing focus on targeted phishing attacks against key executives to secure credentials for thefts against corporate assets."[35] In particular, analysts were seeing reports that company executives were receiving "specially targeted emails that attempt to do two things: 1) Install malware [malicious code] to give the phisher access to the corporations' systems and 2) Gain access to the corporations' bank accounts."[36]

- **Use of Malicious Code.** In January 2004, the APWG reported that "[t]he majority of phishing attacks use a link to a website as their 'call to action', although a few attacks ask the recipient to download a file (that generally contains a virus or Trojan program [i.e., a Trojan horse program, which appears to have a benign function but actually contains some form of malicious computer code])."[37] In these few instances, the APWG, added,

> A small number of phishing attacks [i.e., 5] include a Trojan attachment in the message that recipients are encouraged to download and run. These Trojans generally contain keylogger programs that silently monitor the victim's computer for patterns of keystrokes that look like credit card numbers or social security numbers, or for new windows that open containing the name of a bank or credit card company. The program captures the typed information to a text file, and then uses a built-in email system to send the contents to an email dropbox for collection.[38]

By November 2007, APWG data indicate that the use of phishing-based Trojan horses and keyloggers has become a principal weapon in the phishing arsenal. In that month, the APWG found 3,500 Uniform Resource Locators (URLs)[39] on which malicious code applications that seek to obtain computer users' passwords were found.[40] The APWG

---

[35] *Id.* at 3.

[36] *Id.*

[37] *See* APWG JANUARY 2004 TRENDS REPORT, *supra* note 29, at 3.

[38] *Id.* at 4.

[39] A URL is the online address of a website, document, or other resource on the World Wide Web. A URL address consists of two parts: (1) a protocol identifier (e.g., http or ftp) that indicates what Internet protocol to use in accessing that address; and (2) a resource name that specifies the Internet protocol (IP) address or domain name where the resource is located. *See* Webopedia, http://www.webopedia.com.

[40] *See* APWG NOVEMBER 2007 TRENDS REPORT , *supra* note 30 at 7.

also found that the top ten countries with websites hosting either phishing-based keyloggers or Trojan downloaders that downloads a keylogger were: (1) United States (68.93 percent): (2) Russian Federation (13.88 percent); (3) China (7.88 percent); (4) Republic of Korea (1.77 percent); (5) United Kingdom (1.67 percent); (6) Poland (1.53 percent); (7) Germany (1.38 percent); (8) France (1.13 percent); (9) Morocco (0.94 percent); and (10) Romania (0.89 percent).[41]

In addition, in November 2007 the APWG found 338 unique password-stealing malicious code applications. This number represents a slight decrease from the number of unique password-stealing malicious code applications in October 2007 (359), but is still the highest number of such applications in a single month since January 2007 (345).[42]

The APWG also reported that it was observing a high increases in "traffic redirectors" (i.e., malicious code that is designed to redirect an Internet user's network traffic to a location where it was not intended to go). The highest volume of these traffic redirectors, according to the APWG, is in malicious code that modifies a user's DNS (i.e., Domain Name System) server settings or hosts file to redirect either certain specific DNS lookups or all DNS lookups to a fraudulent DNS server. The fraudulent server replies with valid responses for most domains, but modifies the name server response to direct the user to certain fraudulent sites (e.g., phishing websites designed to look like the financial institutions where the user does his or her banking). As the APWG explains, "[t]his is particularly effective because the attackers can redirect any of the users requests at any time and the end-users have very little indication that this is happening as they could be typing in the address on their own and not following an email or Instant Messaging lure."[43]

Each of these four trends is of substantial concern to corporate entities and law enforcement agencies in both Canada and the United States. The latter trend, the increased use of malware and infection of websites, is a particular source of concern. Consistent with the APWG findings, one leading information security vendor recently reported that it was seeing 6,000 new infected webpages every day. Moreover, it indicated that less than 20 percent of these websites were hacker sites (i.e., sites crated with malicious intent); 83 percent were legitimate websites that an unauthorized third party had compromised.[44]

---

[41] *See id.* at 8.

[42] *Id.* at 7.

[43] *Id.* at 8.

[44] *See* SOPHOS, SECURITY THREAT REPORT at 2 (2008), *available at* http://www.sophos.com/security/whitepapers/sophos-security-report-2008.

In response to the dramatic growth of phishing attacks, numerous financial institutions' websites in Canada and the United States now include specific warnings to banking customers about phishing, as well as guidance on how to report possible phishing attacks.[45] Law enforcement also increasingly includes warnings about phishing on websites and in special online reports to the general public.[46] In addition, both financial institutions and law enforcement agencies issues special advisories to the public when specific Phishing attacks are being directed at those institutions or agencies.[47]

(2) Other Identity Theft Techniques

Law enforcement authorities in both countries have observed that criminals use a wide variety of identity theft techniques, ranging from high-tech approaches such as phishing to low-tech approaches. Here are some of the more prominent techniques seen in both countries:[48]

- **"Dumpster Diving."** One of the simplest identity theft techniques that continues to be used in some locations is "dumpster diving": i.e., the retrieval of discarded documents, such as payment receipts or bank statements, from trash receptacles and dumpsters.

- **Employee/Insider Theft or Compromise of Data**. Employees in companies, financial institutions, or government agencies may steal or share sensitive personal data from worksites and use it themselves or sell those data to or share it with outsiders.

- **"Shoulder Surfing."** In public areas such as airports, ATM machines, and hotels, criminals will stand near telephone banks or ATM machines that consumers are using

---

[45] *See, e.g.*, CIBC, E-mail Fraud (Phishing), *available at* http://www.cibc.com/ca/legal/phishing-info.html; MBNA Canada, Fraud Reporting & Prevention, available at http://www.mbna.ca/fraud_protect.html; RBC, Email and Website Fraud (Phishing), *available at* http://www.rbc.com/security/bulletinPhishing.html.

[46] *See, e.g.*, BINATIONAL WORKING GROUP ON CROSS-BORDER MASS-MARKETING FRAUD, SPECIAL REPORT ON PHISHING (October 2006), available at http://www.usdoj.gov/opa/report_on_phishing.pdf;

[47] *See, e.g.*, *Beware phishing scam, TD Canada Trust warns customers*, CBC News, Jul 31, 2007, *available at* http://www.cbc.ca/technology/story/2007/07/31/tech-td-phishing.html; U.S. Dep't of Justice, Alert About Hoax Emails (January 30, 2008), *available at* http://www.usdoj.gov/hoaxemail.htm.

[48] *See, e.g.*, PRESIDENT'S IDENTITY THEFT TASK FORCE, COMBATING IDENTITY THEFT: A STRATEGIC PLAN at 14-18 (April 2007), available at http://www.idtheft.gov; Public Safety Canada, Advice for consumers: Identity theft, http://www.publicsafety.gc.ca/prg/le/bs/consumers-en.asp.

and try to see or hear any valuable data that the consumers are using (e.g., credit-card numbers or PIN codes for ATMs).

- **"Skimming."** Skimming may be considered a high-tech variant of shoulder surfing, in which criminals use electronic devices known as "skimmers" to capture the data on the magnetic stripes on the backs of payment cards. There are two principal types of skimmers currently in use: hand-held and non-portable. Hand-held skimmers are used by service workers in various types of retail businesses such as bars and restaurants. When a customer gives the worker his or her payment card, the worker can swipe the card through the legitimate business's swipe-card machine, then swipe the same card through the hand-held skimmer and provide the skimmer and all its captured data at a later date to other criminals. When a non-portable skimmer is mounted over the card slot on an ATM machine, the customer unwittingly sets the skimming process in motion by dipping his card into the slot. The criminals' skimmer reads the customer's magnetic stripe data first, then the legitimate financial institution's card-reader technology recognizes the customer's card and PIN number and effects the transaction. To capture the PIN number, the criminals sometimes use pinhole cameras mounted near the ATM's keypad so that the criminals can see and record the PIN numbers as ATM customers type in the numbers.[49]

- **Theft of Payment Cards and Documents from Personal Areas**. Identity thieves often resort to simple techniques, including theft of wallets or purses from places over which individuals cars and fitness centers and theft of incoming or outgoing mail. Incoming mail may include preapproved credit-card offers, which the identity theft can use to apply for cards in others' names and change the delivery address so the identity theft victim never receives any mail that would alert him to the issuance of cards that he did not request. Outgoing mail may include checks and payment invoices that the criminal can use to obtain access to a victim's bank or financial accounts.

b. Uses of Others' Identifying Data

As indicated earlier, criminals can use stolen or fraudulently obtained personal data in numerous ways to commit fraud and conceal their true identities, while falsely throwing suspicion on the victims whose data they have wrongly used. As the Royal Canadian Mounted Police have noted, once an identity thief has obtained a victim's data, he "can take over the

---

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

victim's financial accounts, open new bank accounts, transfer bank balances, apply for loans, credit cards and other services, purchase vehicles, take luxury vacations, and so on."[50]

One significant trend in the online use of identity theft victims' data is the creation of "botnets" (i.e., networks of computers over which a criminal has taken control through hacking of those computers or introduction of malicious code into those computers). Once a criminal has amassed a botnet, he can use computers in that botnet to carry out a wide range of activity, such as emailing large volumes of spam to prospective victims, conducting denial-of-service attacks, disseminating malicious code, and supporting phishing attacks.[51] A number of information security experts affiliated with the SANS Institute, a leading information security training organization, concluded that the increasing sophistication and effectiveness of botnets will be one of the top online security threats in 2008.[52]

---

[50] Royal Canadian Mounted Police, Identity Theft, *available at* http://www.rcmp-grc.gc.ca/scams/identity_theft_e.htm.

[51] *See, e.g.*, Kelly Martin, *Stop the bots*, SecurityFocus, April 18, 2006, *available at* http://www.securityfocus.com/columnists/398/1.

[52] *See* SANS Institute, Press Release (January 14, 2008), *available at* http://www.sans.org/press/top10menaces08.php.

Section II: The Binational Response to Mass-Marketing Fraud, 2004-2008

Since the 2003 report, Canada and the United States have continued to provide vigorous support for a binational response to the increasingly varied problem of mass-marketing fraud. This Section of the Report will review changes in each country's significant substantive and procedural laws, task forces and strategic partnerships devoted to mass-marketing fraud, approaches to public education and prevention measures, and

A. Substantive and Procedural Laws

1. Canada

Since 2003, the most substantial proposed change in Canadian law pertinent to mass-marketing fraud involves identity theft. Recognizing that identity theft has become a fast-growing problem throughout North America, in November 2007 the Canadian Minister of Justice and Attorney General of Canada Rob Nicholson tabled legislation in the Canadian Parliament that would make it a crime to obtain, possess or traffic in other people's identity information if it is to be used to commit a crime.

The essential purpose and features of the proposed legislation are as follows:

The misuse of another person's identity information, generally referred to as identity fraud, is covered by current offences in the *Criminal Code*, such as personation and forgery. But the preparatory steps of collecting, possessing and trafficking in identity information are generally not captured by existing offences. The proposed legislation would create three new offences directly targeting aspects of the identity theft problem, all subject to five-year maximum sentences:

- obtaining or possessing identity information with intent to use it to commit certain crimes;
- trafficking in identity information with knowledge of or recklessness as to its intended use in the commission of certain crime; and
- unlawfully possessing and trafficking in government-issued identity documents.

Additional *Criminal Code* amendments would create new offences of fraudulently redirecting or causing redirection of a person's mail, possessing a counterfeit Canada Post mail key and possessing instruments for copying credit card information, in addition to the existing offence of possessing instruments for forging credit cards.

Moreover, a new power would also be added permitting the court to order, as part of a sentence, that an offender be required to pay restitution to a victim of identity theft or identity fraud where the victim has incurred expenses related to rehabilitating their identity, such as the cost of replacement cards and documents and costs in relation to correcting their credit history.[53]

2. United States

One significant piece of U.S. legislation affecting mass-marketing fraud that was enacted since 2003 is the U.S. SAFEWEB Act.[54] This legislation provides the FTC with a number of significant sources of authority relating to cross-border fraud enforcement, including the following:

- It authorizes the FTC to disclose certain privileged or confidential information to foreign law enforcement agencies;

- It authorizes the FTC, upon written request, to provide investigative assistance to a foreign law enforcement agency that states it is investigating or enforcing proceedings against violations of laws prohibiting fraudulent or deceptive commercial practices or other practices substantially similar to practices prohibited by laws administered by the FTC, other than federal antitrust laws, without requiring that the conduct identified constitute a violation of U.S. laws;

- It directs the FTC to (1) transmit to the Attorney General evidence of a violation of federal criminal law by any domestic or foreign person, partnership, or corporation, and (2) ensure, with respect to memoranda of understanding and international agreements, that material obtained from foreign law enforcement agencies may be used for investigation, prosecution, or prevention of U.S. criminal law violations;

- It authorizes the FTC to designate its attorneys to assist the Attorney General with litigation in foreign courts and to reimburse the Attorney General for the retention of foreign counsel for such litigation on matters in which the FTC has an interest;

---

[53] Department of Justice Canada, Press Release (November 21, 2007), *available at* http://www.justice.gc.ca/en/news/nr/2007/doc_32178.html.

[54] Pub. L. No. 109-455, 120 Stat. 3372 (December 22, 2006), *available at* http://www.ftc.gov/ogc/FTC_Act_IncorporatingUS_SAFE_WEB_Act.pdf

- It specifies conditions under which an FTC-designated custodian is authorized to share certain compelled or confidential material with foreign law enforcement agencies that certify that the material will be maintained in confidence and will be used only for official law enforcement purposes, and exempts from public disclosure requirements of the Freedom of Information Act any material received by the FTC from foreign sources in the course of an investigation; and

- It authorizes the FTC to (1) retain employees of foreign government agencies on a temporary basis; (2) detail FTC employees to work for foreign agencies; (3) under the Right to Financial Privacy Act of 1978, share information with specified financial and market regulators; and (4) accept payment from a domestic or foreign law enforcement agency for FTC expenses and unconditional gifts, donations, bequests of property, and voluntary services.[55]

In addition, the United States, like Canada, is seeking additional legislation relating to identity theft. In April 2007, as part of a comprehensive national strategy for combating identity theft,[56] the President's Identity Theft Task Force recommended a number of changes in federal criminal law, including the following:

- Amending federal criminal restitution statutes to ensure that identity theft victims can recover for the value of the time they have spent in trying to remediate the harms they suffered;

- Amending the federal identity theft offense[57] and aggravated identity theft offense[58] to ensure that identity thieves who misappropriate information belonging to corporations and organizations can be prosecuted;

- Adding new crimes to the list of predicate offenses for aggravated identity theft;

---

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

[56] *See* PRESIDENT'S IDENTITY THEFT TASK FORCE, COMBATING IDENTITY THEFT: A STRATEGIC PLAN (2008), *available at* http://www.idtheft.gov.

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

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

- Amending the federal criminal statute pertaining to theft of electronic data[59] by eliminating the current requirement that the information must have been stolen through interstate communications;

- Penalizing creators and distributors of malicious spyware and keylogging software by amending the federal statute pertaining to theft of electronic data; and

- Amending the federal cyber-extortion statute[60] to cover additional types of cyber-extortion.[61]

This proposed legislation is now under active consideration in the U.S. Congress.

B. Task Forces and Strategic Partnerships

One of the cornerstones of the binational response to mass-marketing fraud over the past decade has been the establishment of binational task forces and strategic partnerships dedicated to combating mass-marketing fraud. Since 1998, when the first of these binational task forces, Project COLT in Montreal, was established, both countries have now set up six regional task forces and strategic partnerships: Project COLT; the Toronto Strategic Partnership; Project Emptor (Vancouver); the Alberta Partnership (Alberta); the Atlantic Provinces; and the Vancouver Strategic Alliance.

Each of these task forces and partnerships includes representatives of multiple Canadian and U.S. law enforcement agencies. Agencies represented on one or more of the task forces and strategic partnerships include the British Columbia Business Practices and Consumer Protection Authority, the City of Montreal Police Service, the Competition Bureau Canada, the Department of Homeland Security (Immigration & Customs Enforcement), the FBI, the FTC, the Ontario Ministry of Consumer and Commercial Relations, the Ontario Provincial Police, the Royal Canadian Mounted Police, the Sûreté du Québec, the Toronto Police Service, the United Kingdom Office of Fair Trading, the U.S. Attorney's Offices for the Central District of California and the Southern District of Illinois, and the U.S. Postal Inspection Service. These task forces and strategic partnerships continue to play a critical role in combating cross-border

---

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

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

[61] *See* PRESIDENT'S IDENTITY THEFT TASK FORCE, *supra* note 56, at 7, 9.

mass-marketing fraud, with respect not only to coordinated enforcement actions (see below) but also to public education and prevention measures and disruption of criminal operations.

C. Consumer Reporting and Information-Sharing Systems

1. Canada

In Canada, one vital resource for consumer reporting and information-sharing on mass-marketing fraud is PhoneBusters, the national Canadian Anti-fraud Call Center. PhoneBusters is managed

> on a tripartite basis by the Ontario Provincial Police, the Royal Canadian Mounted Police (RCMP) and the Competition Bureau Canada. PhoneBusters plays a key role in educating the public about specific fraudulent telemarketing pitches. The call centre also plays a vital role in the collection and dissemination of victim evidence, statistics, documentation and tape recordings which are made available to outside law enforcement agencies.[62]

PhoneBusters has been providing, and continues to provide, an important resource, both for consumers who wish to report telemarketing fraud, Nigerian fraud, or identity theft and for Canadian and U.S. law enforcement agencies that can draw on the information for analytical and investigative purposes.

Another highly valuable resource with respect to cross-border fraud, including Internet-related fraud, is the RCMP-established initiative known as Reporting Economic Crime On-Line (RECOL). RECOL involves an integrated partnership between international, federal, and provincial law enforcement agencies and with regulators and private commercial entities that have a legitimate investigative interest in receiving copies of complaints of economic crime. RECOL also provides real-time data pertaining to current fraud trends, as well as support for education, prevention, and awareness of economic crime.[63]

---

[62] The Canadian Anti-Fraud Call Centre, PhoneBusters, About Us, *available at* http://www.phonebusters.com/english/aboutus.html.

[63] *See* RECOL, *available at* https://www.recol.ca/intro.aspx?lang=en.

A third system that has been valuable for cross-border fraud cooperation is CANSHARE. CANSHARE is

> an internet-based information-sharing system developed by and for the use of federal and provincial consumer law enforcement agencies. By reducing duplication and increasing the speed and efficiency of information exchange between jurisdictions, [it] enables consumer law enforcement agencies to effectively allocate resources resulting in enhanced consumer protection programs. [It] also allows jurisdictions to monitor and analyze marketplace trends, identify and locate alleged wrongdoers and issue alerts warning of possible deceptive practices in the marketplace.[64]

Since being launched in 1998, CANSHARE was implemented by the federal government, all provinces, and two territories (i.e., theYukon and Northwest Territories).[65]

2. United States

For complaints about all types of consumer fraud, the principal national mechanism for receiving complaints and making complaint data available to law enforcement continues to be Consumer Sentinel. Consumer Sentinel is a complaint database that the FTC has maintained since 1997. Consumer Sentinel collects information about consumer fraud and identity theft from the FTC and over 125 other organizations and makes those data available to law enforcement partners across the United States and around the world for use in their investigations. The Sentinel database now includes more than 4.3 million complaints.[66] Complaints about identity theft filed with the FTC are accessible through the FTC's Identity Theft Data Clearinghouse.

For complaints about Internet-related crime, another vital resource for law enforcement and the public is the Internet Crime Complaint Center (IC3). IC3 is a partnership of the FBI and a nonprofit private-sector entity, the National White Collar Crime Center. IC3 takes and analyzes online complaints from the public and provides a central referral mechanism for law

---

[64] Consumer Measures Committee, Cooperative Enforcement - Working Group, *available at* http://cmcweb.ca/epic/site/cmc-cmc.nsf/en/fe00030e.html.

[65] *See* Service Alberta, Press Release, *available at* http://www.servicealberta.gov.ab.ca/987.cfm.

[66] *See* 2007 FTC COMPLAINT DATA, *supra* note 16, at 2.

enforcement agencies at the state, national, and international levels. IC3 also provides periodic warnings to the public about specific types of online crime.[67]

Since the 2003 report, another initiative that can be of substantial value in mass-marketing fraud investigations is the National Cyber-Forensics and Training Alliance (NCFTA). The NCFTA is a nonprofit organization that provides a neutral collaborative venue where critical confidential information about cyber incidents can be shared discreetly, and where resources can be shared among industry, academia and law enforcement.[68] This unique partnership has been of substantial assistance to multiple federal law enforcement agencies in pursuing complex fraud investigations that involve online activity by criminals. For example, in connection with the 2005 Hurricane Katrina that devastated much of the U.S. Gulf Coast, the NCFTA provided critical assistance in reviewing large quantities of computer-related data to identify websites that potentially were engaging in fraudulent solicitations fo funds for Katrina victims.

D. Enforcement Accomplishments

1. Telemarketing Fraud

Since 2003, the various binational task forces and strategic partnerships, as well as their participating agencies, have brought a number of significant criminal and civil enforcement actions directed at cross-border telemarketing fraud. Here are some examples of those actions:

- *U.S. v. Bellini et al. (C.D. Cal., indictment filed December 19, 2007).* In this case, on December 19, 2007, 22 defendants were indicted on federal fraud-related criminal charges for their roles in an extensive Montreal-based cross-border telemarketing fraud scheme. Members of the fraud operation allegedly

> contacted victims, the majority of whom were elderly, and falsely informed them that they had won large sums of money in a lottery or sweepstakes. The telemarketers allegedly told the victims that they would have to pay various fees or taxes – and in at least one case, money to rent an armored car that would be used to deliver sweepstakes winnings – to obtain their winnings. However, the indictment charges, none of the victims had won any money or would receive any money from the

[67] *See* Internet Crime Complaint Center, *available at* http://www.ic3.gov/.

[68] *See* National Cyber-Forensics and Training Alliance, *available at* http://www.ncfta.net/default2.asp.

telemarketing organization. All of the money sent by victims to pay for the alleged fees was used by the various defendants for their own enjoyment.[69]

One of the defendants, the organizer and leader of the telemarketing organization, allegedly was responsible for obtaining equipment and facilities necessary for the operation of the organization, obtaining "leads" (i.e., listings of victim identifying and contact information) for his telemarketers, obtaining and providing cellular telephones for telemarketers' use, arranging for training of new members of the organization, bringing telemarketers together to "pitch" victims, providing for the collection of money that the victims sent, converting the checks obtained as a result of the organization's fraudulent activities into Canadian dollars, and distributing those funds to himself and other members of the organization. Other members of the organization allegedly made the actual phone calls to victims. Five of the defendants allegedly operated money transfer stores, specifically Western Union and MoneyGram, where some of the victims were instructed to wire money. With these contacts at the money transfer outlets, members of the organization could shield their identities by directing the victims to wire money to aliases, such as "Glen Ross."[70]

The indictment was the direct result of an eight-month investigation by Project COLT. In the course of that investigation, nearly 200 police officers in Canada conducted approximately 50 searches, primarily in the Montreal region, and the FTC contacted nearly 400 U.S. consumers to obtain victim declarations. Canadian authorities also arrested twenty of the 22 defendants later charged in the U.S. indictment. Eighty percent of the transactions reportedly were completed through money transfer sites based in Montreal. Law enforcement authorities estimated that the organization, which primarily conducted fraudulent lottery schemes and fraudulent offers of loans and grants, had been grossing between $5 million and $10 million annually since 2003.[71]

- *U.S. v. Okuomose (C.D. Cal., arrested Nov. 6, 2007)/FTC v. B.C. Ltd. 0763496, d.b.a. Cash Corner Services, Inc. Et al., Civil Action No. C07-1755 RSM (W.D. Wash., preliminary injunction entered November 13, 2007).* In this joint investigation by Project EMPTOR, a British Columbia resident was arrested by RCMP officers pursuant to a provisional arrest warrant based on a criminal complaint filed in U.S. District Court in Los Angeles. The defendant was wanted in connection with his involvement in a fraudulent lottery scheme victimizing U.S. residents that he operated under the name "Cash Corner Services" in British Columbia.

---

[69] U.S. Attorney's Office, Central District of California, Press Release (December 19, 2007), *available at* http://www.usdoj.gov/usao/cac/pressroom/pr2007/163.html.

[70] *See id.*

[71] *See* Royal Canadian Mounted Police, "C" Division, Press Release (January 4, 2008), *available at* http://www.rcmp-grc.gc.ca/qc/comm/2008/01/080104_e.htm.

> According to the complaint, the scheme was carried out by mailing letters advising victims they were lottery winners. The letters instructed victims that, in order to receive their lottery winnings, a fee was required . The complaint alleges that counterfeit checks were also enclosed with each letter which victims were instructed to use to help pay the required fees. Contact numbers listed on the correspondence would connect victims to telemarketers who confirmed that the victim had won the money, but that a fee was required in order to successfully retrieve the funds. Some victims did not receive a letter but only telephone calls from telemarketers who convinced them to send money to the lottery companies, according to the complaint. Victims were asked to send fees ranging from approximately a few thousand dollars to $24,000. After sending the money, victims attempted to deposit their checks and learned that the checks were worthless. No victims interviewed to date have received any money promised to them.[72]

In parallel civil actions, the FTC filed a civil action against the defendant, a relative of the defendant, Cash Corner Services, and another Canadian company, charging them with violations of the Federal Trade Commission Act and the FTC Telemarketing Sales Rule, and obtained a preliminary injunction. In addition, the British Columbia Business Practices and Consumer Protection Authority filed civil actions against the defendants, seeking to freeze their Canadian-based assets.[73]

It should be noted that the FTC staff used provisions of the U.S. SAFEWEB Act to assist Canadian enforcement agencies by sharing key information obtained in the FTC's investigation for use in the related Canadian law enforcement investigation.[74]

- *U.S. v. Porcelli (S.D. Ill., sentenced October 29, 2007).* In this case, on October 29, 2007, the defendant was sentenced to13 years imprisonment for his role in a telemarketing fraud scheme that defrauded individuals throughout the United States of approximately $12 million. The scheme, which targeted people previously rejected for credit cards with fraudulent credit-card offers, operated out of Florida and Utah and utilized U.S. outbound call centers in seven U.S. states; outbound call centers in Grenada,

---

[72] FBI, Press Release (November 6, 2007), *available at* http://losangeles.fbi.gov/pressrel/2007/la110607a.htm.

[73] *See* FTC, Press Release (November 19, 2007), *available at* http://www.ftc.gov/opa/2007/11/cashcorner.shtm.

[74] *See id.*

St. Lucia, and St. Vincent; an outbound call center in Toronto, Canada; and outbound call centers in India.[75]

- *Mass-Marketing Fraud Searches (Montreal, October 9, 2007).* On October 9, 2007, representatives of Project COLT conducted a number of searches in Montreal, in connection with a telemarketing fraud operation that reportedly victimized approximately 1,500 people. The operation's dialers used several pitches, including (1) selling first-aid kits to businesses under the false pretenses that they represented a federal health agency and that businesses were required to have such kits on their premises; (2) selling paper products in the guise of an office supplies dealer; and (3) promoting sales of business listings in business directories, but failing to include those listings in the directories that were delivered. Victims of the scheme were principally small- and medium-sized businesses in Canada, the United States, and Europe.[76]

- *U.S. v. Kimoto (S.D. Ill., indictment filed June 20, 2007).* In this case, on June 20, 2007, a St, George, Utah and Las Vegas resident was indicted on various federal offenses arising out of an alleged telemarketing fraud scheme that fraudulently offered credit cards to individuals who previously had been turned down for credit cards. The indictment alleges that the scheme operated out of Utah and utilized a network of U.S. outbound call centers that the defendant organized in seven U.S. states; Caribbean outbound call centers in Grenada, St. Lucia, and St. Vincent; an outbound call center in Toronto, Canada; and outbound call centers in India. The indictment alleges that the scheme victimized more than 300,000 consumers throughout the United States, in an amount of approximately $43 million.[77] The defendant and his companies had previously been the subject of an FTC enforcement action that resulted in, among other things, judicial imposition of a receivership and a monetary judgment of $106 million against the defendant and one of his companies.[78]

---

[75] *See* U.S. Attorney's Office, Southern District of Illinois, Press Release (October 29, 2007), *available at* http://www.usdoj.gov/usao/ils/press/2007/Oct/10292007_Porcelli_press%20release.htm.

[76] *See* Royal Canadian Mounted Police, "C" Division, Press Release (October 9, 2007), *available at* http://www.rcmp-grc.gc.ca/qc/comm/archives/2007/10/071009_e.htm.

[77] *See* U.S. Attorney's Office, Southern District of Illinois,, Press Release (June 20, 2007), *available at* http://www.usdoj.gov/usao/ils/press/2007/Jun/06202007_Kimoto%20press%20release.htm.

[78] *See* Final Monetary Judgment As To Defendants Kyle Kimoto and Assail, Inc., FTC v. Assail, Civil Action No. W-03-CA-007 (W.D. Tex., September 24, 2004), *available at* http://www.ftc.gov/os/caselist/assail/050124kimoto.pdf.

- *U.S. v. Brown and Love (W.D.N.Y., guilty pleas entered March 29, 2007).* In this case, two Las Vegas residents pleaded guilty to federal criminal charges involving laundering the proceeds of illegal telemarketing activity in Canada. According to the U.S. Attorney's Office that prosecuted the case, in April 2004 one of the defendants met an individual online who identified herself as "Missy Young" of Ontario, Canada. "Young" (a false name) told that defendant that she and others in Canada were involved in telemarketing activities, and needed people in the United States to open bank accounts through which the proceeds of the telemarketing could be processed and sent back up to Canada. Between June 2004 and January 2005, the first defendant opened seven bank accounts at various banks, using various business names. That defendant enlisted the other defendant to open another two bank accounts. During this same period, the first defendant transferred and transmitted approximately $802,000 in U.S. funds to the telemarketers in Canada, including "Young," through wire transfers to bank accounts controlled by the telemarketers in the United States and Canada. The telemarketers also obtained funds from these bank accounts through ATM withdrawals made in the United States and in Canada. During the same period, and in the same manner, the second defendant transferred and transmitted approximately $630,700 in U.S. funds from her accounts to the telemarketers in Canada.

  The underlying telemarketing activity in Canada involved illegal schemes to obtain money by means of false and fraudulent pretenses and representations. Telemarketers in Canada allegedly contacted U.S. citizens and sold them a product or service for approximately $300. Based on the alleged sale, the telemarketers in Canada would create a "preauthorized draft check" and deposit it into one of the bank accounts that the defendants opened. It was part of the telemarketing fraud scheme that the personal and bank data put on the "preauthorized draft checks" – including the account holder's name, address, checking account number and bank routing number, -- was obtained through fraud, in that a large percentage of the checks were generated without the knowledge or permission of the person fraudulently identified as the "purchaser."[79]

2. Internet Fraud

The following are examples of cross-border Internet fraud prosecutions:

- *U.S. v. Hendricks (D. Ore., sentenced February 25, 2007).* In this case, on February 25, 2007, a Florida man was sentenced to six years imprisonment after pleading guilty to several federal criminal offenses relating to his role as the head of an investment fraud

[79] *See* U.S. Attorney's Office, Western District of New York, Press Release (April 2, 2007), *available at* http://www.usdoj.gov/usao/nyw/press/press_releases/BROWNANDLOVEPRESS.pdf.

business which took in approximately $13 million from more than 1,500 victims throughout the United States and Canada. The defendant admitted that he used a company he and another individual had formed, Pacific Achievements International (PAI), to solicit investment funds through false statements and promises, primarily through the Internet. He falsely represented to investors that PAI would be a network marketing business and promised investors that if they invested with PAI, they would be sent a fast start bonus and significant profits.

Based upon these false promises and representations, investors transferred more than $13 million into PAI bank accounts in Oregon, Washington, and Florida, that the defendant and another individual controlled. The defendant and another PAI promoter diverted more than $2 million in PAI money to support their personal livestyles, including the use of $1.6 million for the purchase of personal residences in Florida and Washington. Knowing that PAI was not generating any income, the defendant and another PAI promoter tried to recover funds by unsuccessfully investing PAI money in high yield investment scams in Beirut, Lebanon, the Bahamas, Nevada and Texas. They lost $2.7 million in PAI money in these other scams. The defendant ultimately pleaded guilty to conspiracy to commit mail and wire fraud, wire fraud, and failing to file a U.S. income tax return.[80]

- *U.S. v. Kraser (S.D. Fla., sentenced May 7, 2006).* In this case, a defendant was sentenced to 21 months in prison for fraudulently soliciting charitable donations supposedly intended for Hurricane Katrina relief. According to the indictment, the defendant falsely claimed in online conversations, and on a website at www.AirKatrina.com, that he was piloting flights to Louisiana to provide medical supplies to the areas affected by Hurricane Katrina and to evacuate children and others in critical medical condition. He also claimed that he had organized a group of Florida pilots to assist him in his supposed relief efforts.[81] In only two days, the defendant collected approximately $40,000 from 49 people in the United States, Canada, Mexico, Europe, and Hong Kong, with one contributor donating $20,000.[82]

3. Nigerian Fraud

---

[80] *See* U.S. Attorney's Office, District of Oregon, Press Release (February 25, 2007), *available at* http://portland.fbi.gov/dojpressrel/2007/investmentscheme022507.htm; U.S. Attorney's Office, District of Oregon, Press Release (October 24, 2006), *available at* http://portland.fbi.gov/dojpressrel/2006/investmentfrau102406.htm.

[81] *See* U.S. Attorney's Office, Southern District of Florida, Press Release (May 8, 2006), *available at* http://miami.fbi.gov/dojpressrel/pressrel06/mm050806.htm.

[82] *See* FBI, Busted for Katrina Fraud (October 21, 2005), *available at* http://www.fbi.gov/page2/oct05/katrinaescam102105.htm.

As indicated above, Nigerian-led fraud operations are becoming a more substantial threat to consumers in both Canada and the United States. Recent significant law enforcement actions relating to Nigerian fraud operations include the following:

- *U.S. v. Anisiobi et al. (E.D.N.Y., guilty pleas entered January 30, 2008).* On January 30, 2008, three defendants, who had been extradited from the Netherlands to the United States for their roles in a Nigerian fraud ring operating from Amsterdam, pleaded guilty to various counts of conspiracy, wire fraud, and mail fraud. According to the indictment and an earlier filed complaint,

  > the defendants sent spam to thousands of potential victims, in which they falsely claimed to control millions of dollars located abroad. Attempting to conceal their identities, the defendants used a variety of aliases, phone numbers, and email addresses. In one scenario, the defendants sent emails purporting to be from an individual suffering from terminal throat cancer who needed assistance distributing approximately $55 million to charity. In exchange for a victim's help, the defendants offered to give a 20% commission to the victim or a charity of his or her choice. Subsequently, as part of the ruse, the defendants would send a variety of fraudulent documents, including a "Letter of Authority" or a "Certificate of Deposit," making it appear that the promised funds were available, and pictures of an individual claiming to suffer from throat cancer. [One defendant] allegedly telephoned victims, disguising his voice to give the impression that he was suffering from throat cancer.
  >
  > After obtaining their victims' trust, the defendants asked them to wire-transfer payment for a variety of advance fees, ostensibly for legal representation, taxes, and additional documentation. In return, the victims received nothing. In a variation of the scheme, if the victims said they could not afford to pay the advance fees, the defendants would send them counterfeit checks, supposedly from a cancer patient, to cover those fees. Many victims deposited the checks and then drew on them to wire-transfer the advance fees. Subsequently, when the checks did not clear, the victims suffered substantial losses.[83]

- *R. v. Anigozie et al. (Ontario, arrested November 2, 2007).* In this investigation, three Ontario residents were arrested in connection with the production and mass mailing of counterfeit checks throughout North America. The investigation was primarily focused on the "lab" where the fraudulent checks were being manufactured. Counterfeit checks and supporting documentation were allegedly being prepared in regard to fraudulent

[83] *See* U.S. Attorney's Office, Eastern District of New York, Press Release (January 30, 2008), *available at* http://www.usdoj.gov/usao/nye/pr/2008/2008jan30.html.

statements regarding charities, lotteries, and personal loans. Police also executed five search warrants and seized several computer systems, printers, scanners, counterfeit U.S. currency, and thousands of checks in various stages of production.[84]

- *U.S. v. Roberts (S.D. W. Va., sentenced January 2006).* In this case, the defendant was sentenced to 18 months imprisonment for his role in a scheme to distribute counterfeit checks to others. At the time of his arrest, the defendant was found to be in possession of counterfeit checks and money orders totaling more than $680,000. He later told law enforcement agents that he had met a person named "John" on the Internet, and that he had received the counterfeit checks and money orders from "John," as well as envelopes, UPS postage, and directions on how to distribute the checks to various individuals.[85]

4. Identity Theft

The following are several examples of criminal enforcement actions that have been brought since 2003 against criminals engaging in identity theft with cross-border aspects:

- *U.S. v. Hardiman (W.D.N.Y., sentenced September 12, 2007).* In this case, on September 12, 2007 a Toronto resident was sentenced to two years imprisonment for aggravated identity theft. The defendant, who trafficked in counterfeit credit cards, sold counterfeit credit cards and driver's licenses over the Internet. The counterfeit credit cards used the numbers of actual accounts issued by financial services entities, including Wachovia, Visa, and American Express. In addition, for the counterfeit drivers' licenses he produced, the defendant used actual driver's license numbers belonging to other individuals from the Canadian Provinces the licenses were purportedly issued. Both the U.S. Secret Service and the Toronto Police Service took part in the investigation.[86]

- *U.S. v. Ciocan and Pasca (W.D. Pa., indictment filed May 8, 2007).* In this case, two Romanian nationals living in Canada were indicted on federal charges of conspiracy, bank fraud, and aggravated identity theft for their roles in an identity theft scheme that involved acquiring bank customers' identifying data at ATM terminals. According to the charges in the case, the defendants allegedly

> participated in a scheme in which members of the scheme installed, on Automated Teller Machines, card readers that

---

[84] *See* Ontario Provincial Police, Press Release (November 2, 2007).

[85] *See* U.S. Attorney's Office, Southern District of West Virginia, Press Release (January 11, 2006), *available at* http://www.usdoj.gov/usao.wvs/press_releases/2006/jan06/011106.html.

[86] *See* U.S. Attorney's Office, Western District of New York, Press Release (September 12, 2007), *available at* http://www.usdoj.gov/usao/nyw/press/press_releases/HardimanSentencing.pdf.

> surreptitiously stole the account and other information from the ATM cards without the card users' knowledge or consent. Members of the conspiracy also fraudulently obtained the personal identification numbers associated with the cards. Members of the conspiracy then used the account information stolen from the ATM cards to manufacture counterfeit ATM cards. [The defendants allegedly] then traveled from city to city using the counterfeit ATM cards and the fraudulently obtained personal identification numbers to withdraw funds from various ATM machines.[87]

- *Internet-Based Identity Theft Charges (Ontario, charges laid March 2006).* In this case, Ottawa police uncovered an Internet-based identity theft scheme that targeted applicants for a job posting that was published online. Members of the scheme reportedly notified a prospective victim that he or she was a suitable candidate for the $70,000-a-year position, and asked the prospective victim to fill out an application form and to send a $20 processing fee. Once the victims submitted their personal information, the criminals used that information to apply for credit cards and identification and social insurance cards in the victims' names. Two suspects were arrested after Ottawa police executed a search warrant at a residence, seizing approximately 60 credit cards, social insurance cards and driver's licences from both Ontario and Quebec. Authorities alleged that the suspects had been operating the scam since 2002.[88]

E. Public Education and Prevention Accomplishments

Since 2003, Canadian and U.S. law enforcement authorities have continued to carry out a variety of approaches to foster improved public education and awareness about mass-marketing fraud. These include:

- **Disruption of Criminal Activity**. In late 2007, Project COLT, after learning that certain envelopes addressed to locations in the United States contained marketing fraud materials, conducted a one-month surveillance operation that led to the discovery of more than 50,000 fraudulent letters addressed to U.S. and some Canadian citizens in an attempted fraud of nearly $195 million. The letters included counterfeit checks with face

---

[87] U.S. Attorney's Office, Western District of Pennsylvania, Press Release (October 9, 2007), *available at* http://pittsburgh.fbi.gov/dojpressrel/2007/identitytheft050907.htm.

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

amounts ranging from $2,000 to $5,000. The results of this operation provided an opportunity for the RCMP to warn the public about the seizure and the fraud schemes it had uncovered.[89]

Other kinds of efforts to disrupt criminal mass-marketing fraud operations can also provide benefits for victims. Since 1998, for example, Project COLT has recovered more than $20 million for mass-marketing fraud victims.

- **Public Advisories.** Various agencies in both countries have issued public advisories to warn the public about particular types of mass-marketing fraud activity, such as the use of counterfeit checks and money orders in fraud schemes[90] and spam falsely claiming to be sent by a law enforcement agency.[91]

- **Public Education Campaigns and Advertisements.** In 2007, the RCMP and other law enforcement agencies outside North America participated in an initiative led by the U.S. Postal Inspection Service to warn the public about the risks of counterfeit checks in fraud schemes. The educational components of this initiative included public-service advertisements on television and in print media and a website, created by the National Consumers League, with additional educational resources.[92] This initiative also involved substantial collaboration between the public and private sectors – including seven leading financial-services businesses and associations and Publishers Clearing House -- in supporting and publicizing the advertising campaign.[93]

  The FTC has conducted numerous public education measures and events related to mass-marketing fraud. For example, in 2006, the FTC and the U.S. Food and Drug Administration, working with government agencies in Canada and Mexico, launched a drive to stop deceptive online advertisements and sales of products misrepresented as cures or treatments for diabetes. As of October 2006, the joint campaign had included

---

[89] *See* RCMP, "C" Division, Press Release (December 18, 2007), *available at* http://www.rcmp-grc.gc.ca/qc/comm/archives/2007/12/071218_e.htm.

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

[91] *See, e.g.*, U.S. Secret Service, FRAUDULENT SPAM E-MAIL CLAIMING TO BE FROM THE U.S. SECRET SERVICE (January 26, 2007), *available at* http://www.secretservice.gov/fraud_email_advisory.shtml.

[92] *See* fakechecks.org, *available at* http://www.fakechecks.org/.

[93] *See* fakechecks.org, About Us, *available at* http://www.fakechecks.org/links.html.

approximately 180 warning letters and other advisories sent to online outlets in the three countries.[94] Also in 2006, the FTC held a Hispanic Fraud Prevention Forum in New York City. The forum featured the announcement of new consumer education materials, and outreach partnerships with schools in New York City, as well as the results of a Hispanic Multi-Media Surf that the FTC and 60 partners in the United States and Latin America conducted.[95]

In Montreal, Canada, Project COLT initiated a public education campaign targeted specifically at potential telemarketing boiler room employees. In a series of advertisements and flyers aimed at students, Project COLT warned of the dangers of working for fraudulent businesses. Project COLT also encouraged students to report suspicious activities to law enforcement.

In 2005, the FTC, with significant contributions from DOJ, the United States Postal Inspection Service, other federal agencies, and numerous private groups, launched "On Guard Online," (www.onguardonline.gov) an interactive website that provides tips for consumers about a variety of mass-marketing frauds including identity theft, phishing, spyware, spam scams, and VoIP.

Most recently, in February 2008, the U.S. Postal Inspection Service conducted a nationwide campaign to heighten public awareness about identity theft. As part of that campaign, the Postmaster General sent out 121 million letters to every household in the United States that included an FTC brochure on identity theft.

March is Fraud Prevention Month. In Canada, during March, the Fraud Prevention Forum[96], chaired by Competition Bureau Canada, leads a concerted fraud awareness campaign. Through a wide variety of communications media and activities, the more than one hundred private and public sector organization members of the Forum deliver millions of messages to educate and alert the public about the dangers of fraud.

---

[94] *See* Food and Drug Administration, Press Release (October 19, 2006), *available at* http://www.fda.gov/bbs/topics/NEWS/2006/NEW01494.html.

[95] *See* FTC, Press Release (September 27, 2006), *available at* http://www.ftc.gov/opa/2006/09/nyworkshop.shtm.

[96] *See* 2008 Fraud Prevention Month Campaign and Fraud Prevention Forum membership *available at* http://www.competitionbureau.gc.ca/epic/site/cb-bc.nsf/en/h_00122e.html

Section III: Continuing Challenges in Mass-Marketing Fraud - Refining the Binational Action Plan

Since the 2003 Report, Canada and the United States have continued to make substantial strides in binational cooperation to combat cross-border fraud, particularly mass-marketing fraud. Thanks to their respective law enforcement authorities, additional joint task forces and strategic partnerships have been established, and investigations and prosecutions of leading offenders in mass-marketing fraud schemes successfully pursued.

At the same time, both countries' experiences with mass-marketing fraud since 2003 provide substantial evidence that continuing collaboration and sharing of scarce resources to combat the problem is essential. On an ongoing basis, law enforcers, prosecutors, and regulators in both countries will need to decide what new steps can and should be taken to become even more effective in combating cross-border fraud schemes.

To provide a coherent framework for the steps needed to improve binational effectiveness in combating cross-border fraud, the 2003 Report presented an Action Plan that outlined key measures to strengthen existing binational capabilities to combat the most significant types of cross-border fraud that affect both countries. This Action Plan addressed strategic and operational concerns regarding investigation, prosecution, and public education and prevention of cross-border fraud schemes.

A. The Binational Action Plan for Cross-Border Fraud

The 2003 Action Plan consisted of 12 points grouped under five principal headings. This Section of the Report will discuss what steps have been taken, and still need to be taken, since the 2003 Report to carry out each of these recommendations and to offer an additional recommendation to meet the evolving threats that mass-marketing fraud poses for both countries.

1. Strategies

(1) ***Both countries should compare their respective strategies against cross-border telemarketing fraud and ensure harmonization of those strategies in addressing newer developments in telemarketing fraud.***

Since the 2003 Report, various members of national-level working groups in both countries, including this Subgroup and the Canadian Mass Marketing Fraud Strategy Working Group, have discussed their current strategic frameworks in greater detail and identify areas where greater harmonization of those strategies would be in order. With the completion of the Mass Marketing Fraud Strategy Group's work on a national strategy, as described below,

agencies in both countries should be able to coordinate their respective strategies even more closely.

(2) ***As part of that process of harmonization, both countries should also examine their existing national-level working groups that address other types of cross-border fraud issues, and where appropriate take similar steps to ensure harmonization of national strategies in addressing those types of fraud.***

Since the 2003 Report, in 2005 Canadian law enforcement partners established the National Mass Marketing Fraud Strategy Working Group. This working group, which drew on the expertise and advice of numerous Canadian and U.S. law enforcement agencies, identified a "four pillar" strategy for controlling, dismantling and neutralizing the criminal activities of mass marketing fraud operations in Canada and internationally. The four pillars of this strategy are: (1) more vigorous law enforcement; (2) increasing public awareness and reporting; (3) creating tougher sanctions and more targeted legislation; and (4) increased information sharing and cooperation.[97] The adoption and full implementation of this strategy will necessarily require continued and close coordination between Canada and the United States on strategic and tactical approaches to combating mass-marketing fraud of all types.

2. Operational Efforts

(3) ***Agencies that are members of existing interagency telemarketing fraud task forces should reaffirm their commitment to participation in those task forces, and consider inclusion of new agencies where appropriate to obtain additional investigative resources against cross-border fraud.***

Since the 2003 Report, as described earlier, there are now six active Canadian-based task forces and strategic partnerships directed at mass-marketing fraud. Although some agencies no longer participate in certain task forces and partnerships, the operations of the task forces and partnerships since 2003 provide substantial and concrete evidence that they continue to make very substantial contributions to the fight against cross-border mass-marketing fraud. Continuation of those efforts is dependent on key participants in those task forces and partnerships continuing their membership and, as appropriate, attracting additional law enforcement or regulatory members at all levels of law enforcement to enhance their capabilities as mass-marketing fraud schemes continue to evolve.

(4) ***In investigating and preparing to prosecute cases against particular cross-border fraud schemes for prosecution, police, law enforcement agents, and prosecutors should explore all***

---

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

avenues for seizing and forfeiting proceeds of the crimes traceable to those schemes and returning as much money as possible in restitution to victims of the schemes.

Since the 2003 Report, law enforcement authorities in both countries have shown greater interest in making use of their respective legal procedures for tracing, seizing, and forfeiting the proceeds of major mass-marketing fraud schemes. While the opportunities and capabilities for seizing and forfeiting mass-marketing fraud proceeds will necessarily vary from case to case, law enforcement and prosecutive agencies should continue to incorporate consideration of seizure and forfeiture into their strategic planning of particular cases, and use all available legal authority as appropriate in those cases.

(5) ***In investigating cross-border fraud cases, prosecutive offices in both countries should continue to examine the speed with which mutual legal assistance requests are processed and carried out, and to look for ways of expediting the processing of such requests.***

Since the 2003 Report, the Cross Border Crime Forum has taken up this issue directly and assigned it to the Prosecutions Subgroup for further action. That Subgroup in turn has been systematically examining the problems associated with timely assistance under the Canada-U.S. Mutual Legal Assistance Treaty (MLAT) and extradition treaty.

(6) ***Prosecutors and civil enforcement agencies in both countries should consider whether to use "sweeps" - a series of coordinated enforcement actions against similar types of criminal or fraudulent activities – in selected categories of cross-border fraud cases.***

Since the 2003 Report, law enforcement authorities in both countries have spearheaded two major multinational sweeps directed at specific categories of mass-marketing fraud. First, in the U.S. Attorney General, together with Canadian and other law enforcement officials, announced "Operation Roaming Charge." This operation, which the U.S. Attorney General and other U.S. and Canadian law enforcement officials announced on October 5, 2004, was the most extensive multinational enforcement operation ever directed at domestic and international telemarketing fraud operations. The nine-month operation involved more than 100 separate investigations that led to the discovery of more than five million victims, who suffered losses totaling more than $1 billion. It resulted in the arrest of more than 100 individuals in the United States, and an additional 35 arrests in other countries; the execution of more than 190 U.S. and Canadian search warrants; the conviction of 70 individuals by the date of the operation's announcement; and the filing by state attorneys general of 279 criminal, civil and regulatory actions against illegal telemarketing operations.[98]

More recently, on May 23, 2006, the U.S. Attorney General and other law enforcement officials announced the results of Operation Global Con. This operation, which ran for 15

[98] *See* U.S. Dep't of Justice, Press Release (October 5, 2004), *available at* http://www.usdoj.gov/opa/pr/2004/October/04_crm_680.htm.

months in 2005 and 2006, was the largest and most far-reaching multinational enforcement operation ever directed at mass-marketing fraud schemes. In this operation, 96 separate U.S. investigations in this operation led to the discovery of more than 2.8 million victims, who suffered losses totaling more than $1 billion. It resulted in the arrest of 139 individuals in the United States, and an additional 426 arrests in Canada, Costa Rica, the Netherlands, and Spain; the execution of 447 search warrants in those five countries; 61 convictions as of the date of the announcement; and the filing of 20 civil actions by the FTC against 140 defendants.[99]

Sweeps such as Roaming Charge and Global Con offer significant benefits to law enforcement in several respects. Apart from the immediate opportunities that they provide for public education messages, these operations also demonstrate the value of sustained long-term planning, information-sharing, and coordination among law enforcement agencies in multiple countries. If they are to have the maximum impact on international mass-marketing fraud, law enforcement agencies will need to pool their intelligence and enforcement resources efficiently to identify and pursue the most significant mass-marketing fraud operations and their ringleaders, while generating additional valuable criminal intelligence that benefits governments in their enforcement and education efforts. As circumstances permit, investigative and prosecutive agencies in both countries should consider organizing and conducting other enforcement sweeps against mass-marketing fraud schemes, and to engage other countries as appropriate in those sweeps, to increase the impact of their efforts.

(7) ***Law enforcement agents and prosecutors in both countries should explore how to make more effective use of videoconferencing technology to obtain needed testimony from witnesses in the United States.***

Since the 2003 Report, both countries have found that videoconferencing continues to have the same potential values and limitations (e.g., logistical complexities and cost) for testimony in Canadian proceedings. U.S. agencies should therefore be prepared to respond when needed to Canadian requests for assistance with remote testimony from U.S. residents, and to coordinate with each other as appropriate to distribute the potential burden of providing such support on a case-by-case basis.

3. Information Sharing

(8) ***Both countries should take steps to facilitate the prompt sharing, both at national levels and among existing and future interagency task forces, of public information about enforcement actions against cross-border fraud schemes that law enforcement, prosecutive, and regulatory agencies in either country have taken, including information about the impact of those schemes on individuals and businesses.***

---

[99] *See* U.S. Dep't of Justice, Press Release (May 23, 2006), *available at* http://www.usdoj.gov/opa/pr/2006/May/06_crm_321.html.

Since the 2003 Report, both countries have made only limited progress towards this goal. While Canada and the United States have individually made more information available to the general public about their respective enforcement efforts against mass-marketing fraud, they need to develop more systematic approaches and mechanisms to share such information on a timely basis among law enforcement agencies in both countries and in other countries. Both countries have initiated the process of developing such approaches and mechanisms, and have identified several promising practices for that purpose.

(9) ***Both countries should coordinate their efforts to contact other countries whose citizens are being targeted in cross-border fraud schemes, to share information and training opportunities with appropriate government agencies in those countries, and to take specific steps toward expanded cooperation and coordination with those countries in investigating and prosecuting such schemes.***

Since the 2003 Report, both countries have taken several steps to coordinate with several other countries, such as Australia, New Zealand, and the United Kingdom. As this Report has shown, the effects of cross-border fraud schemes increasingly are being felt beyond North America. Residents of the United Kingdom, Australia, and New Zealand are now being targeted, as residents of Canada and the United States have been. Law enforcement agencies in both countries should share information about which points of contacts in other countries would be the most suitable for coordinated outreach on cross-border fraud issues, and engage in coordinated outreach to exchange information about fraud issues and explore ideas for further information-sharing, training, and other cooperative ventures.

4. Coordination Between Public and Private Sectors

(10) ***Both countries should coordinate their efforts to consult with entities in the financial services and electronic payments industries about specific measures to reduce the use of particular payments mechanisms by cross-border fraud schemes.***

Since the 2003 Report, various agencies in both countries have taken the initiative to consult with private-sector financial entities about the exploitation of specific payments mechanisms, such as money transfer businesses and electronic funds transfers. To date, however, both countries have not yet carried out this recommendation for binational coordination on such consultations. Governments in both countries would benefit from coordinating their efforts in this regard, particularly with reference to the abuse of payment mechanisms such as money transfer businesses and payment processors and the growing use of counterfeit checks in mass-marketing schemes.

5. Training

(11) ***Both countries should plan to have at least one conference each year at which investigators and prosecutors can exchange information about current trends and***

developments in cross-border fraud and receive training about investigative techniques and substantive and procedural laws that have proven effective against major fraud schemes.

Since the 2003 Report, both countries have continued to have annual conferences to discuss trends and developments in cross-border fraud and provide training on legal and investigative approaches to such cases. Most recently, in February 2008, the Alberta Partnership Against Cross Border Fraud , in partnership with the National Mass Marketing Fraud Strategy Working Group in Canada and the Canadian Anti-Fraud Call Center (PhoneBusters) held an International Investigators' Skills Development Workshop in Banff, Alberta. The workshop, which featured speakers from numerous Canadian, U.S., and other law enforcement agencies, was attended by more than 200 participants. In addition, the U.S. Department of Justice's National Advocacy Center, on roughly an annual basis, has conducted training seminars on international white-collar crime that has been available to non-U.S. law enforcement representatives. Because participants in these conferences and seminars uniformly find that they have appreciable value for investigators and prosecutors, both countries should continue the practice of annual conferences and explore additional opportunities to share information on mass-marketing fraud trends and training.

(12) ***Both countries should also explore the use of videoconferencing for joint binational or multinational training on specific fraud-related topics.***

Both countries, as outlined in the 2003 report, have made use of videoconferencing for training purposes. Both the United States and Canada are willing to continue to use videoconferencing for these purposes in the future.

B. Further Recommendation

(13) Both countries should enhance their capabilities to assemble criminal intelligence on emerging trends in mass-marketing fraud and to share that intelligence, consistent with applicable legal requirements, with each other and with additional countries' law enforcement agencies.

As certain aspects of international mass-marketing fraud – among others, the continuing growth and expansion of Nigerian-led criminal groups' engagement in a wide variety of mass-marketing schemes – become apparent to law enforcement agencies, law enforcement in both countries need to move promptly in identifying what types of criminal intelligence will be most useful to them in responding to those trends, and how that intelligence can best be amassed, analyzed, and disseminated in useful forms to other interested law enforcement and regulatory agencies. While each country must be sensitive to all applicable domestic legal constraints on information-gathering and -sharing, law enforcement authorities must work within those constraints to improve their effectiveness in combating the dominant and emerging strains of mass-marketing fraud. Recent experience has shown, in a number of mass-marketing fraud investigations and prosecutions, that mass-marketing fraud enforcement depends on enhancing multinational, not merely binational, cooperation.

* * *

In their first ten years of formal binational cooperation, Canada and the United States have laid a firm foundation – through information-sharing, disruption of criminal activity, public education and prevention, and enforcement – to combat all forms of mass-marketing fraud more effectively than ever before. Maintaining and strengthening that foundation will be essential to both countries' responses to the evolving threat that mass-marketing fraud continues to pose to consumers, commercial entities, and governments alike.