Solicitor General Canada | Solliciteur général Canada

Mass-Marketing Fraud

A Report to the Attorney General of the United States
and the Solicitor General of Canada

May 2003

⁂

Binational Working Group on
Cross-Border Mass-Marketing Fraud

Table of Contents

Executive Summary

Section I: Mass-Marketing Fraud Today

Telemarketing Fraud

- Cross-border telemarketing fraud remains one of the most pervasive forms of white-collar crime in Canada and the United States. The PhoneBusters National Call Centre estimates that on any given day, there are 500 to 1,000 criminal telemarketing boiler rooms, grossing about $1 billion a year, operating in Canada. (3)

- Several types of cross-border telemarketing fraud have increased substantially from 1997 to 2002: fraudulent prize and lottery schemes; fraudulent loan offers; and fraudulent offers of low-interest credit cards or credit-card protection. (3)

- Seven trends in cross-border telemarketing fraud since 1997 are especially noteworthy:

  - *(1) Types of Telemarketing Fraud "Pitches".* The most prevalent among Canadian-based telemarketing fraud operations are fraudulent offers of prizes or lotteries; fraudulent loan offers; and fraudulent offers of low-interest credit cards or credit-card protection. (5)
  - *(2) Methods of Transmitting Funds.* Criminal telemarketers generally prefer their victims to use electronic payment services, such as Western Union and Travelers Express MoneyGram, to send funds for the promised goods or services. Some operations are moving back to greater use of the mails (such as Express Mail) and making more use of bank-to-bank transfers, to obtain victims' funds. Law enforcement agencies are seeing more telemarketing schemes, such as those offering "guaranteed" credit cards, make substantial use of Automated Clearing House (ACH) processes to debit consumers' bank accounts. (10)
  - *(3) Methods of Laundering Fraud Proceeds.* A number of cross-border telemarketing schemes have been using more complex and sophisticated methods of laundering the proceeds they receive from victims. (10)
  - *(4) Involvement of Organized Crime.* Law enforcement agencies are seeing a growing involvement of organized criminal groups in Canadian-based

cross-border telemarketing fraud operations. They report that some groups are using proceeds from fraudulent telemarketing to fund other illegal activities such as narcotics, gun running, and prostitution. Many telemarketing fraud operation managers and employees, as well as Western Union agents, have been threatened, extorted, and assaulted. (11)

- *(5) Dispersion of Telemarketing Fraud Operations Within Canada.* Many telemarketing fraud operations no longer co-locate the components of their schemes in a single location. Law enforcement agents also have seen a trend among fraudulent telemarketing operations to establish greater specialization and division of functions among the operations' personnel. Finally, a number of operators are moving their "boiler room" or administrative operations into provinces other than the ones where the three telemarketing fraud task forces are based (i.e., Québec, Ontario, and British Columbia). (12-13)
- *(6) Concealment Techniques.* Many criminal telemarketers use extraordinary measures to conceal their day-to-day operations and to make investigating and proving the fraudulent schemes more difficult. These include the use of cell phone and prepaid calling cards that can be easily discarded; stolen identity cards; multiple mail drops; and impersonation of law enforcement agents. (13)
- *(7) Expansion of Victim Targeting Beyond North America.* A number of Canadian-based telemarketing fraud operations are looking beyond North America, and are increasingly targeting residents of the United Kingdom,[1] Australia, and New Zealand. (14)

Internet Fraud

- The number of fraud-related complaints of all types that consumers file with the FTC is rising significantly: from 107,890 in 2000 to 133,891 in 2001 to 218,284 in 2002. Moreover, the percentages of these complaints that involve Internet-related fraud are also rising significantly: from 31 percent in 2000 to 42 percent in 2001 and 47 percent in 2002. (15)

---

[1] *See* PhoneBusters, News Release, *Lottery Scam Tricks Britons* (May 9, 2002) (reprinted from BBC Radio Five Live), http://www.PhoneBusters.com/Eng/Charges_Arrests/May_9_2002_1a.html.

- Both the numbers and relative percentages of Internet-related cross-border fraud complaints have been steadily increasing in the past three years. Internet-related fraud complaints (excluding identity theft) rose from 12,213 in 2000 (22 percent of all cross-border fraud complaints) to 16,318 in 2001 (32 percent of all cross-border fraud complaints), then nearly doubled to 30,798 in 2002 (34 percent of all cross-border fraud complaints). (15)

Identity Theft

- U.S. and Canadian data show that identity theft has become one of the fastest-growing forms of crime in Canada and the United States. (16)

- Identity thieves acquire other people's identifying data in many different ways. These include theft or diversion of mail; recovery of trash; electronic "skimming" or "swiping" of credit cards; and compromise of government or company employees with access to valuable data, such as employee databases and consumer credit reports; and theft or "hacking" of company databases. (17)

- Identity theft is never committed for its own sake. Criminals engage in identity theft because the acquisition of other people's identifying data enables them to engage in a growing variety of other criminal acts, such as fraud, organized crime, and terrorism. (20)

Africa-Related Fraud Schemes

- Solicitations that offer bogus opportunities to assist persons in Africa in laundering illegal proceeds or transferring other funds out of Africa have been a longstanding problem for law enforcement in Canada, the United States, and the United Kingdom. (23)

- These types of solicitations were the leading source of U.S. consumers' cross-border fraud complaints about companies in other foreign countries, according to U.S. Federal Trade Commission data. (24)

Section II: The Response to Mass-Marketing Fraud, 1998-2003

- Both Canada and the United States have carried out all of the recommendations made in November 1997 to the fullest extent possible under respective national laws and legal processes. (26)

- These include:
  - Changes in substantive and procedural laws (27);
  - Establishment of multiagency task forces and strategic partnerships – Project COLT in Québec, the Toronto Strategic Partnership in Ontario, Project Emptor in British Columbia, and the FBI's Operation Canadian Eagle – which have been highly productive in conducting investigations that led to criminal prosecutions and other enforcement actions (30);
  - Consumer reporting and information-sharing systems, such as the PhoneBusters National Call Centre, RECOL, and Canshare in Canada, and Consumer Sentinel and the Internet Fraud Complaint Center in the United States (35);
  - Enforcement actions in both Canada and the United States against various forms of mass-marketing fraud (41); and
  - Public education and prevention measures, such as reverse boiler rooms, interception and return of victim proceeds, public advisories, public service announcements and campaigns, and public-private sector partnerships. (46)

Section III: Current Challenges in Cross-Border Fraud - Towards A Binational Action Plan

- Canadian and American law enforcement have reached "the end of the beginning" in combating cross-border mass-marketing fraud. Law enforcers, prosecutors, and regulators in both countries should now decide what new steps can and should be taken to become even more effective in combating cross-border fraud schemes. (56)

- This Report presents a twelve-point Action Plan to provide a coherent framework for those steps. This Action Plan outlines key measures to strengthen

existing binational capabilities to combat the most significant types of cross-border fraud that affect both countries. (56)

- *(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.* (57)
- *(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.*
- *(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.* (57)
- *(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 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.* (58)
- *(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.* (60)
- *(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. (61)*
- *(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.* (63)
- *(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.* (64)
- *(9) Both countries should coordinate their efforts to contact other countries whose citizens are being targeted 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. (65)

- *(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.* (65)
- *(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.* (66)
- *(12) Both countries should also explore the use of videoconferencing for joint binational or multinational training on specific fraud-related topics.* (67)

- Each of these measures, taken separately, offers some benefits for law enforcement and the public in both countries. In combination, they provide a substantial foundation for binational cooperation that can substantially reduce the scope and severity of cross-border mass-marketing fraud. (68)

* * *

Introduction

Throughout North America, legitimate businesses, non-profit organizations, and government agencies routinely use mass-marketing techniques, including bulk mailing, telemarketing, and the Internet, to contact prospective customers, investors, or contributors. The effectiveness of mass-marketing techniques, however, is not limited to legitimate business. Criminals in Canada and the United States increasingly are turning those techniques into weapons directed at the public.

Today, mass-marketing fraud – a general term for frauds that exploit mass-communication media, such as telemarketing fraud, Internet fraud, and identity theft – is widely prevalent in Canada and the United States. Statistical data and investigative information from law enforcement in both countries show that mass-marketing fraud is a significant and growing problem.

In telemarketing fraud, for example, several types of cross-border telemarketing fraud have increased substantially from 1997 to 2002.[2] In Internet fraud, the number of fraud-related consumer complaints – and the percentage of those complaints that involve Internet-related fraud – are rising appreciably.[3] In identity theft, identity-theft complaints to the U.S. Federal Trade Commission (FTC) have increased fivefold in just the last three years, reaching 161,819 in 2002.[4] In other types of mass-marketing fraud, such as Africa-related fraud schemes (e.g., "4-1-9" schemes), annual losses from these schemes are estimated to be in the hundreds of millions of dollars.[5]

Law enforcement authorities in both countries are seeing cross-border aspects in many of the mass-marketing fraud schemes that they investigate. The number of cross-

---

[2] *See* PhoneBusters, *Statistics on Phone Fraud: United States* (updated as of January 12, 2003), http://www.PhoneBusters.com/Eng/Statistics/index_us.html.

[3] *See* FEDERAL TRADE COMMISSION, NATIONAL AND STATE TRENDS IN FRAUD AND IDENTITY THEFT, JANUARY - DECEMBER 2002 at 3 (January 22, 2003) [hereinafter "FTC, NATIONAL/STATE TRENDS"].

[4] *See id.* at 8.

[5] *See* Brian McWilliams, *Nigerian Money Scams Thrive On The Internet*, NEWSBYTES, February 20, 2002.

border fraud-related complaints in the FTC's Consumer Sentinel database has increased exponentially, from only 84 in 1995 to 4,567 in 1997 and 30,798 in 2002.[6] Cross-border telemarketing fraud remains highly active – and in some respects has become a greater concern for law enforcement, due to the growing involvement of organized crime in such schemes. At the same time, Internet fraud and identity theft operations routinely have cross-border features that increase the difficulties of successful investigation and enforcement action. Other mass-marketing frauds, such as Africa-related advance-fee schemes, are becoming more pervasive – due to the use of mass e-mails – and capable of harming victims in many countries around the world.

Canada and the United States first undertook a thorough examination of certain cross-border fraud issues in 1997. In response to a directive by then-President Bill Clinton and Prime Minister Jean Chrétien, a binational working group was formed to examine the problem of cross-border telemarketing fraud. That working group provided the President and the Prime Minister with a detailed report and recommendations that laid the groundwork for substantial improvements in enforcement capabilities and binational coordination and cooperation in combating telemarketing fraud.[7]

---

[6] *See* FEDERAL TRADE COMMISSION, CROSS-BORDER FRAUD TRENDS: JANUARY - DECEMBER 2002 at 5 (2002) [hereinafter "FTC, CROSS-BORDER FRAUD TRENDS"], http://www.ftc.gov/bcp/conline/edcams/crossborder/PDFs/Cross-BorderCY-2002.pdf. Some of this increase reflects better publicity regarding complaint mechanisms, an increase in the number of sources contributing data to Consumer Sentinel, and an increase in overall complaints since 1995. Nonetheless, the percentage of complaints with a cross-border element has increased from less than 1 percent in 1995 to 11 percent in 2001, 12 percent in 2001, and 14 percent in 2002. FTC data may actually underestimate the percentage of cross-border complaints. Data about company locations is taken from consumer complaints. Consumers may not realize that in some cases, the company address they have been given is only a mail drop in the United States and not the physical location of the company. In other cases, the consumer may not know or may not have reported whether the location is in the United States or abroad.

[7] *See* BINATIONAL WORKING GROUP ON CROSS-BORDER TELEMARKETING FRAUD, UNITED STATES - CANADA COOPERATION AGAINST CROSS-BORDER TELEMARKETING FRAUD: REPORT TO PRESIDENT BILL CLINTON AND PRIME MINISTER JEAN CHRÉTIEN at 7 (November 1997) [hereinafter "1997 REPORT"].

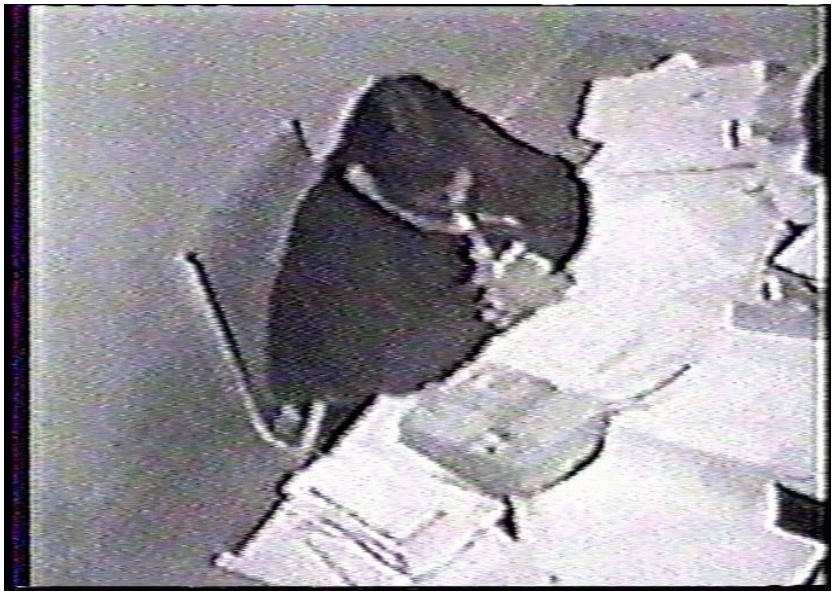
In the five years since the Working Group's report, there have been substantial changes in both governments' responses to cross-border telemarketing fraud schemes, and changes in the methods and techniques that criminals are using in those and other mass-marketing fraud schemes. These changes make it appropriate to review the current state of developments in cross-border mass-marketing fraud of all types; to note the extent of implementation of the 1997 Report's recommendations; to identify significant changes in the organization and operation of cross-border fraud schemes; and to note possible areas for legal, policy, operational, and administrative improvements. This Report will address each of these topics.

The Report will first describe the current state of mass-marketing fraud affecting Canada and United States. It will then summarize the principal legal, policy, operational, and administrative changes that have occurred in both countries since 1997 in response to telemarketing fraud and other mass-marketing fraud. This summary will include (1) substantive and procedural laws; (2) multiagency task forces and strategic partnerships; and (3) noteworthy enforcement and public education and prevention accomplishments (e.g., examples of significant cross-border prosecutions and public educational efforts). It will then identify certain problems, stemming from changes in cross-border fraud over the past five years, that may require new responses or tools. As the Report will describe, these will include (1) the growth in numbers and locations of various telemarketing and other mass-marketing schemes, (2) the increasing involvement of organized crime (including the use of strongarm tactics in fraud), and (3) the distinctive challenges that identity theft poses for law enforcement and the public. Where appropriate, it will offer specific recommendations for legal, policy, operational, and administrative changes that appear necessary to meet the current challenges of cross-border mass-marketing fraud.

This Report has benefitted from the strong support and contributions of many agencies in both countries that are members of the Binational Working Group or the joint telemarketing task forces operating in Canada. These include (a) federal law enforcement and regulatory agencies, such as the RCMP, the FBI, the Department of the Solicitor General of Canada, the United States Department of Justice, Canadian Customs and Revenue, the Department of Homeland Security's Bureau of Immigration and Customs Enforcement (formerly the United States Customs Service), Canada Post, the United States Postal Inspection Service, the United States Secret Service, the Competition Bureau of Industry Canada, and the FTC; (2) state, provincial, and local law enforcement agencies, such as the Ontario Provincial Police, the Toronto Police Service, and the Sûreté du Québec; and (3) Federal, state, and provincial prosecutive

organizations, such as the United States Attorney's Offices in Los Angeles, Boston, Concord (N.H.), the Ministries of the Attorney General in Ontario, British Columbia, and Québec, and the National Association of Attorneys General.

Section I: Mass-Marketing Fraud Today



A cross-border telemarketer talks with a prospective victim. (Source: U.S. Postal Inspection Service)

This Section will describe the principal types of mass-marketing fraud that have significant cross-border impact in Canada and the United States. At the outset, it is important to note some general data that the FTC recently published on cross-border fraud complaints it received in 2002:

- 46 percent of all cross-border fraud complaints involved U.S. consumers who complained about businesses in Canada.
- 33 percent involved U.S. consumers who complained about businesses in other foreign countries.
- 6 percent involved Canadian consumers who complained about companies in the United States.
- 3 percent involved Canadian consumers who complained about businesses in other foreign countries.
- 12 percent involved foreign consumers who complained about companies in the United States or Canada.[8]

---

[8] *See* FTC, CROSS-BORDER FRAUD TRENDS, *supra* note 6, at 9.

The principal categories of products or services that prompted complaints by U.S. consumers about cross-border fraud in 2002 were foreign money offers (i.e., "4-1-9" schemes) (24 percent), advance-fee loans (24 percent), prizes/sweepstakes/gifts (23 percent), Internet auctions (10 percent), shop-at-home catalog sales (5 percent), lotteries/lottery ticket buying clubs (3 percent), and business opportunities/franchises/distributorships (2 percent).[9] The top five categories of products or services that specifically prompted complaints by U.S. consumers about Canadian companies were advance-fee loans (40 percent of all such complaints about Canadian companies), prizes/sweepstakes/gifts (37 percent), Internet auctions (8 percent), lotteries/lottery ticket buying clubs (4 percent), and shop-at-home/catalog sales (2 percent).[10]

Overall, FTC data show that in 2002, complaints by U.S. consumers against companies located in Canada reported a total of $33,370,902 in losses, with an average amount paid of $2,607. In contrast, in 2002 complaints by U.S. consumers against companies located in other foreign countries reported a total of $38,896,689 in losses, with an average amount paid of $6,782.[11]

---

[9] *See id.* at 11.

[10] *See id.*

[11] *See* FTC, CROSS-BORDER FRAUD TRENDS, *supra* note 6, at 14. Interpretation of these amounts, and the differences between them, is difficult because the dollar loss figures in the FTC data are self-reported by consumers. Many consumers do not report the amount of dollar loss, and some report the amount for which they were solicited but not the amount that they actually paid. This may skew the actual totals of losses and amounts paid.

A. Telemarketing Fraud

Cross-border telemarketing fraud remains one of the most pervasive forms of white-collar crime in Canada and the United States.[12] The PhoneBusters National Call Centre estimates that on any given day, there are 500 to 1,000 criminal telemarketing boiler rooms, grossing about $1 billion a year, operating in Canada.

Complaint data compiled by the U.S. Federal Trade Commission (FTC) show that telemarketing is the most favored means of initiating contact between fraud schemes and victims in Canada and the United States. Among U.S. victims who complained about companies located in Canada, telephone contact far exceeded any other means of initial contact over the past three years. Telephone contact accounted for 63 percent in 2000, 68 percent in 2001, and 66 percent in 2002. By contrast, mail accounted for 17 percent, 13 percent, and 10 percent, respectively; e-mail accounted for 6 percent, 4 percent, and 5 percent, respectively; and Internet website (or other Internet contact) accounted for 7 percent, 7 percent, and 10 percent, respectively.[13]

Data from the PhoneBusters National Call Centre – the call center in Canada for deceptive telemarketing, Internet fraud, identity theft, and Africa-related fraud schemes – show that several types of cross-border telemarketing fraud have increased substantially from 1997 to 2002.[14] Consistent with the trends in the FTC data reported above, complaints of fraudulent prize and lottery schemes to PhoneBusters have more than doubled, from 3,413 in 1997 to 8,077 in 2002. Reports of fraudulent loan offers have nearly doubled, from 2,885 in 1997 to 5,542 in 2002. Reports of fraudulent offers of low-interest credit cards or credit-card protection showed the most drastic increase, from only 60 in 1997 to 3,390 in 2002.

The face of cross-border telemarketing fraud in North America has been evolving over the past five years, as criminals modify their methods and techniques. Certain aspects of fraudulent telemarketing remain largely unchanged. They maintain their bases of operations (including their telephone solicitors) in Canada, but target

---

[12] *See* 1997 REPORT, *supra* note 7, at 1.

[13] *See* FTC, CROSS-BORDER FRAUD TRENDS, *supra* note 6, at 15.

[14] *See* PhoneBusters, *Statistics on Phone Fraud: United States* (updated as of January 12, 2003), http://www.PhoneBusters.com/Eng/Statistics/index_us.html.

prospective victims (often the elderly) in the United States through lists of previous fraud victims (known as "mooch lists" or "sucker lists") that they buy from willing suppliers in the United States. Some also frequently use U.S. mail houses and printers to prepare and mail fraudulent solicitations or "fulfillment packages" (actually premiums or travel packages of little or no actual value) to U.S. victims. Many of these fraudulent schemes continue to make the same basic "pitches" (i.e., fraudulent stories) that were in use in 1997, such as schemes that offer nonexistent prizes, lottery winnings, or investment opportunities.

Finally, many of the schemes operating in the three largest provinces in Canada tend to use the same types of "pitches." Operations in British Columbia tend to concentrate on fraudulent foreign lottery offers, investments in so-called "British bonds," credit-card protection, recovery rooms, and fraudulent billing of compromised credit cards;[15] operations in Ontario tend to concentrate on fraudulent advance-fee loan offers, fraudulent offers of low-interest credit cards or credit-card protection, stock swaps, prizes and sweepstakes, and "investment-grade" gemstones;[16] and operations in Québec tend to concentrate on fraudulent lottery chances, prize offers, and "recovery" schemes (i.e., schemes in which the solicitor pretends to be able to return a portion of the victims' previous fraud losses, but demands advance payment of "taxes" or "fees").[17]

---

[15] *See* Prepared Statement of Mary Ellen Warlow, Acting Deputy Assistant Attorney General, Criminal Division, U.S. Department of Justice, Before the U.S. Senate Permanent Subcomm. on Investigations (June 15, 2001), http://govt-aff.senate.gov/061501_warlow.htm [hereinafter Warlow Statement]. *See also* Prepared Statement of Hugh G. Stevenson, Associate Director, Planning and Information Consumer Protection Bureau, Federal Trade Commission, Before the U.S. Senate Permanent Subcomm. on Investigations (June 15, 2001), http://govt-aff.senate.gov/061501_ftc.htm [hereinafter Stevenson Statement].

[16] *See* Warlow Statement, *supra* note 15; Stevenson Statement, *supra* note 15.

[17] *See id.* FTC data show that in 2002, Ontario had the highest number of complaints by U.S. consumers (7,678), followed by Québec (4,204) and British Columbia (1,208). In Ontario, advance-fee loans accounted for 63 percent of all such complaints; prizes/sweepstakes, 18 percent; Internet auction, 7 percent; and other, 12 percent. In Québec, prizes/sweepstakes accounted for 70 percent of such complaints; advance-fee loans, 9 percent; Internet auction, 5 percent; lotteries, 5 percent; and other, 11 percent.

To understand the significance of the cross-border telemarketing fraud problem today, however, it is important to scrutinize the operational changes that criminals have made since 1997. Seven trends in cross-border telemarketing fraud are especially noteworthy.

1. Types of Telemarketing Fraud "Pitches"

The first trend involves the changes in the "pitches" that criminal telemarketers use to persuade their victims to send money. Certain "pitches" that once were popular, such as fraudulent offers of investment-grade gemstones, are effectively no longer in use. Other "pitches" have shown greater staying power in cross-border schemes. The following, according to data from PhoneBusters and other law enforcement agencies, are the most prevalent among Canadian-based telemarketing schemes:

a. ***Fraudulent Offers of Prizes and Lotteries***. FTC data show that in 2002, 61 percent of U.S. consumers' cross-border fraud complaints about prizes, sweepstakes, and gift offers were against companies located in Canada.[18] PhoneBusters data (set forth below in Table 1) show that reports of fraudulent prize and lottery schemes to PhoneBusters have more than doubled, from 3,413 in 1997 to 8,077 in 2002.. It is important to note that the number of reporting victims, after gradually declining from 1,578 in 1997 to 1,400 in 1999, nearly doubled the next year to 2,955 and increased another 41 percent to 4,181 in 2001. Even though the number of reporting victims declined slightly in 2002 to 3,515, that total is still greater than any other year except 2001 and more than 2.5 times as many victim complaints as in 1999.[19]

In British Columbia, prizes/sweepstakes accounted for 47 percent; Internet auction, 14 percent; lotteries, 9 percent; advance-fee loans, 8 percent; and other, 22 percent. *See* FTC, CROSS-BORDER FRAUD TRENDS, *supra* note 6, at 22.

[18] *See* FTC, CROSS-BORDER FRAUD TRENDS, *supra* note 6, at 20.

[19] *See* PhoneBusters, *Statistics on Phone Fraud: United States* (updated January 12, 2003), http://www.PhoneBusters.com/Eng/Statistics/index_us.html. All losses are listed in U.S. dollars.

Table 1 - U.S. Residents' Reports of Fraudulent Telemarketing Prize and Lottery Solicitations: PhoneBusters, 1997-2002					
Year	*Attempts*	*Victims*	*Total Reports*	*Total Victim Losses Reported*	*Average Loss*
1997	1,835	1,578	3,413	$10,103,170.63	$6,402.52
1998	1,623	1,548	3,171	$10,562,183.37	$6,823.12
1999	1,655	1,400	3,055	$10,212,352.95	$7,294.54
2000	2,631	2,955	5,586	$19,997,216.40	$6,767.25
2001	4,361	4,181	8,542	$22,621,468.70	$5,410.54
2002	4,562	3,515	8,077	$16,542,858.28	$4,706.36

b. ***Fraudulent Loan Offers***. FTC data show that in 2002, 41 percent of U.S. consumers' complaints about advance-fee loan schemes were against companies located in Canada.[20] PhoneBusters data offer even more detail about the growth of advance-fee loan schemes based in Canada. These latter data (set forth below in Table 2) show that reports of fraudulent loan offers have nearly doubled, from 2,885 in 1997 to 5,542 in 2002. After a period from 1998 to 2000 when the number of victims steadily declined from 4,385 to 1,862, the number of victims nearly doubled in 2001 to 3,303 and increased slightly in 2002.[21]

[20] *See* FTC, CROSS-BORDER FRAUD TRENDS, *supra* note 6, at 19.

[21] *See* PhoneBusters, *Statistics on Phone Fraud: United States* (updated January 12, 2003), http://www.PhoneBusters.com/Eng/Statistics/index_us.html. All losses are listed in U.S. dollars.

Table 2 - U.S. Residents' Reports of Fraudulent Loan Solicitations: PhoneBusters, 1997-2002					
Year	*Attempts*	*Victims*	*Total Reports*	*Total Losses Reported*	*Average Loss*
1997	1,129	1,756	2,885	$912,704.74	$519.76
1998	2,339	4,385	6,724	$2,583,278.96	$589.12
1999	1,615	2,424	4,039	$1,488,464.18	$614.05
2000	686	1,862	2,548	$1,077,520.66	$578.69
2001	1,776	3,303	5,079	$2,584,328.74	$782.42
2002	2,126	3,416	5,542	$3,565,473.87	$1,042.76

c. ***Fraudulent Offers of Low-Interest Credit Cards and Credit-Card Protection.*** PhoneBusters data (as shown below in Table 3) show that reports of fraudulent offers of low-interest credit cards or credit-card protection showed the most drastic increase, from only 60 in 1997 to 3,390 in 2002. It is interesting to note that while the average loss per consumer has fluctuated only between $159 and $287 during those six years, after 1997 total reported losses approximately doubled in each successive year.[22] These data suggest that schemes using these pitches are able to defraud more and more consumers each year, as the nature of the scheme – promising but never delivering a credit card or credit-card protection – makes it highly difficult to "load" or "reload" a victim (i.e., to defraud the same victim more than once as part of the same scheme) by offering the victim another credit card.

Law enforcement authorities, however, have found that certain credit-card schemes, by using direct debiting of bank accounts, can accomplish a form of reloading. Using a technique known as "upsales," criminals may charge victims not only for the originally requested credit card, but also for other services that the victims never requested, such as unwanted credit-card protection plans or memberships in automobile clubs. In credit-card protection schemes, financial institutions may also suffer loss when victims challenge the fraudulently induced charges and financial institutions put through chargebacks on behalf of the

[22] *See* PhoneBusters, *Statistics on Phone Fraud: United States* (updated January 12, 2003), http://www.PhoneBusters.com/Eng/Statistics/index_us.html. All losses are in U.S. dollars.

victims. One bank in Montreal reportedly lost approximately US $550,000 in a matter of weeks because of such chargebacks.

Table 3 - U.S. Residents' Reports of Fraudulent Low-Interest Credit Cards and Credit-Card Protection Solicitations: PhoneBusters, 1997-2002

Year	*Attempts*	*Victims*	*Total Reports*	*Total Losses Reported*	*Average Loss*
1997	17	43	60	$8,302.00	$193.07
1998	94	217	311	$34,536.35	$159.15
1999	199	448	647	$79,106.50	$176.58
2000	277	619	896	$145,348.21	$234.81
2001	382	998	1,380	$287,001.94	$287.58
2002	853	2,537	3,390	$555,766.95	$219.06

2. Methods of Transmitting Funds

A second trend involves changes in the methods that criminal telemarketers favor to receive victim's funds. Over time, criminal telemarketers have searched for methods and mechanisms that accomplish two objectives: (1) obtaining victims' money and converting the funds to their own benefit as quickly as possible; and (2) reducing the risk of loss of those funds due to stop-payment orders or chargebacks. Although some telemarketers in Canada and the United States have used charge cards to obtain victim funds, laws and credit-card issuer policies give ample opportunity for consumers to dispute transactions even after the charge has been processed, and to obtain chargebacks that eliminate the charges from their accounts.

Accordingly, in the 1990s many criminal telemarketers began to use commercial courier services so that they could arrange to have victims' payments picked up directly from their homes. This trend may have stemmed from two beliefs: (1) that mail would be more likely to get government scrutiny, by the United States Postal Inspection Service and Canada Post, than commercial courier packages; and (2) that because courier packages do not go through the mail, they would not be subject to the mail fraud statute (18 U.S.C. § 1341). In response, the United States Congress in 1996

amended the mail fraud statute to cover both mail matter and packages delivered by commercial couriers.[23]

Subsequently, through the latter half of the 1990s fraudulent telemarketers made less and less use of both mail and courier delivery, and increasingly had their victims use various forms of electronic payments. Table 4 below sets forth the funds transportation and transfer methods that U.S. victims reported to PhoneBusters from 1996 to 1999.[24] As these data show, use of U.S. Postal Service delivery services (e.g., express, regular, and registered mail) steadily decreased after 1996, use of commercial couriers dropped drastically after 1997.

Table 4 - U.S. Residents' Reports of Methods of Payment Transportation/Transfer to Fraudulent Telemarketers: PhoneBusters, 1996-1999

Year	*Total Reports*	*U.S. Postal Service (all types)*	*Couriers: UPS*	*Couriers: Federal Express*	*Couriers: Other*	*Credit-Card/ Direct Debit/ Wire Transfer*
1996	1,003	197	184	95	19	89
1997	1,297	366	132	144	27	193
1998	1,197	200	63	72	74	352
1999	815	157	25	45	4	397

PhoneBusters data (as set forth in Table 5 below) also show the changes in the methods of payments that criminal telemarketers have directed U.S. victims to use in paying for bogus lotteries, prizes, loans, credit cards, or other services:

---

[23] *See* Pub. L. No. 103-322, § 250006(1), 108 Stat. 2087, 2147 (amending 18 U.S.C. § 1341).

[24] *See* PhoneBusters, Statistics on Phone Fraud (2002), http://www.PhoneBusters.com/Eng/Statistics/index_us.html.

Table 5 - U.S. Residents' Reports of Telemarketing Fraud Victim Payment Methods: PhoneBusters, 1996-1999							
Year	*Total Reports*	*Money Orders (all types, including cashier's checks)*	*Checks (all types)*	*Western Union*	*Credit Card*	*Cash*	*Direct Debit*
1996	1,014	580	70	54	29	13	6
1997	1,305	807	72	134	38	7	8
1998	1,211	476	87	305	35	16	7
1999	821	287	52	343	37	14	7

Law enforcement agents report that criminal telemarketers generally prefer their victims to use electronic payment services, such as Western Union and Travelers Express MoneyGram, to send funds for the promised goods or services. Through cooperative efforts between the private sector and Project COLT, at least 62 persons who were agents for electronic payments services in Québec had their business relationships with those services terminated because of involvement with criminal telemarketers. Some police representatives also report that where criminals perceive that law enforcement is working more closely with electronic payments companies on telemarketing fraud investigations, their telemarketing operations are moving back to greater use of the mails (such as Express Mail) and making more use of bank-to-bank transfers, to obtain victims' funds. Law enforcement agencies are seeing more domestic and cross-border telemarketing schemes, such as those offering "guaranteed" credit cards, make substantial use of Automated Clearing House (ACH) processes to debit thousands of consumers' bank accounts.

3. Methods of Laundering Fraud Proceeds

Law enforcement authorities in both countries have found that a number of cross-border telemarketing schemes they are investigating have been using more complex and sophisticated methods of laundering the proceeds they receive from victims. Once fraudulent telemarketing organizations have their representatives pick up victims' funds from money transfer locations, those funds are often wired offshore and then laundered and returned to Canadian bank accounts. Some investigations have traced proceeds through financial institutions and check-cashing businesses in the

Middle East and other countries outside North America, such as Israel and Jordan. Law enforcement authorities have reason to believe that telemarketing organizations are deliberately using financial institutions in some countries that lack adequate anti-money laundering controls, or that have no formal or informal arrangements for mutual legal assistance with Canada or the United States.

4. Involvement of Organized Crime

One of the more disturbing trends in cross-border telemarketing fraud is the growing involvement of organized criminal groups in Canadian-based telemarketing operations. In Québec, law enforcement authorities have observed that because telemarketing fraud schemes are capable of generating as much as $1 million a week in untaxed profits, members of Hell's Angels (and their lower level affiliates), the Italian Mafia, and additional other criminal groups with other ethnic affiliations have shown great interest in taking over or dominating operations of fraudulent telemarketing firms. Law enforcement agents report that some groups are using proceeds from fraudulent telemarketing to fund other illegal activities such as narcotics, gun running, and prostitution.

In one respect, this should not be wholly surprising. At other times and places, members of organized crime have found that fraud can be vastly more profitable, and may carry far less risk of harm from competitors or risk of substantial sentences, than other types of criminal activity. The growing involvement of such groups in criminal telemarketing however, poses a genuine risk that, in contrast to previous telemarketing fraud operations, they will be more likely to use violence in running the telemarketing schemes or in fending off competition.

There is growing evidence that this risk of violence is becoming quite real:

- Several organized-crime homicides and contracts to commit homicides in the past few years are believed to be linked to the Montreal telemarketing fraud business.

- Law enforcement representatives with Project COLT and the Montreal City Police have also discovered that many telemarketing fraud operation managers and employees, as well as Western Union agents, have been threatened, extorted, and assaulted. In one instance, a Western Union agent had his convenience store destroyed by fire by an organized-crime street gang over telemarketing-fraud

payment issues. Another operator was punched and had his finger broken to entice his cooperation. One organized-crime group extorted a telemarketing operation, threatening the manager with firearms and taking surveillance pictures of his family.

- Firearms are increasingly part of the criminal telemarketer's "tools of the trade." In Ontario, a June 6, 2002 action by the Toronto Strategic Partnership against an organized criminal advance-fee loan group netted 11 persons, 4 guns (including 3 semiautomatic handguns and a sub-machine gun), a machete, a bullet proof "police" vest and police ID, marijuana, and CA $66,000 in cash.

5. Dispersion of Telemarketing Fraud Operations Within Canada

Largely because of the efforts of the binational telemarketing fraud task forces and strategic partnerships in Canada,[25] law enforcement authorities have been seeing three ways in which criminal telemarketing schemes are dispersing their operations. First, many of these schemes no longer follow the traditional business model of co-locating all components of the scheme (i.e., solicitors, customer complaint, and administration) in a single building. Instead, the operators of the scheme may establish their offices in one place, hire solicitors to work out of another place in a different city or province, and set up commercial mailboxes and bank accounts in yet another city or town. In the latter case, the operators may deliberately select a commercial mail business or bank somewhere in the United States, where they wish to convey the impression that their operations are in fact in the United States.

Second, law enforcement agents have seen a trend among fraudulent telemarketing operations to establish greater specialization and division of functions among the operations' personnel. In telemarketing operations of any significant size, specific supervisors are assigned to oversee working groups that will seldom cross over to other areas in the organization. A typical group of supervisors would include the following:

- *Leads Supervisor*. This supervisor will work on obtaining names and telephone numbers of potential victims. Once the sucker lists are obtained, they are given to the telemarketing supervisor.

---

[25] *See* Section II for a discussion of these task forces and strategic partnerships.

- *Telephone Supervisor*. This supervisor will buy cellular telephones, which cannot be traced back to the organization and can be easily discarded after a few weeks of use. Some criminal groups reportedly have even purchased cell phone retail companies and retail stores to ensure a fresh supply of cell phones for the telemarketers.

- *Boiler Room Supervisor*. This supervisor will hire the actual persons who will make the telephone calls to the victims in the United States (and who instruct the victims on where and how to send the monies to Canada).

- *Money Receiver Supervisor*. This supervisor will hire persons to set up mail drops and to receive the funds from the U.S. victims (usually in false names), and will set up bank accounts for bank-to-bank wire transfers.

- *Money Broker Supervisor*. This supervisor will make arrangements to have the monies laundered and converted into Canadian currency.

- *Security*. This supervisor is the "enforcer" for the overall operation, and will ensure that all rules are followed and that no one in the organization talks to law enforcement.

Third, a number of operators are moving their "boiler room" or administrative operations into provinces other than the ones where the three telemarketing fraud task forces are based (i.e., Québec, Ontario, and British Columbia). Their evident purpose is to conduct operations in jurisdictions where they believe there will be less law enforcement and regulatory scrutiny. In part because of their enforcement efforts, Project COLT and Project Emptor have seen evidence of telemarketers' moving from Quebec and British Columbia, respectively into other areas of central and western Canada.

6. Concealment Techniques

Many criminal telemarketers use extraordinary measures to conceal their day-to-day operations and to make investigating and proving the fraudulent schemes more difficult. These measures include, according to a U.S. Department of Justice official,

> using cell phones (sometimes in conjunction with prepaid "calling cards"), which can be discarded after several weeks of intensive use; using stolen

> identity cards to open mail drops for receipt of payments that victims mail to them; using multiple mail drops that shuttle victim-related mail through multiple destinations; [and] impersonation of FBI and Customs agents or RCMP officers, to make victims believe that law enforcement is already aware of their losses . . . .[26]

Agents with Project COLT in Montreal, for example, have found that criminal telemarketers, in pretending to be law enforcement agents, have even set up telephone numbers on which voice-mail recordings falsely indicate that the office in question is "U.S. Customs," "IRS," or a law firm. Postal Inspectors also report that many of these cell phone accounts used by criminal telemarketers are opened in assumed names, and that victims' personal identification is regularly used to open cell phone and mail drop accounts.

7. Expansion of Victim Targeting Beyond North America

As law enforcement authorities continue to investigate and prosecute telemarketing fraud operations based in Canada, a number of these operations are looking beyond the United States to other English-speaking jurisdictions beyond North America. Investigators in both countries are aware that for at least the past year, some telemarketers have been increasingly targeting residents of the United Kingdom,[27] Australia, and New Zealand. These operations typically offer exactly the same kinds of fraudulent lottery and investment "opportunities" that have been directed at Canadian and U.S. residents.

PhoneBusters has counted at least 15 operations targeting the United Kingdom by mail, and 17 operations targeting the United Kingdom by telephone.[28] Similarly, the FTC reports that it has received numerous reports from the United Kingdom's Office of

---

[26] *See* Warlow Statement, *supra* note 15.

[27] *See* PhoneBusters, News Release, *Lottery Scam Tricks Britons* (May 9, 2002) (reprinted from BBC Radio Five Live), http://www.PhoneBusters.com/Eng/Charges_Arrests/May_9_2002_1a.html.

[28] *See* PhoneBusters, *Companies Targeting the U.K*, http://www.PhoneBusters.com/Eng/Charges_Arrests/Companies_People/CompaniestargetingUK.html.

Fair Trading about Canadian-based telemarketing operations targeting United Kingdom consumers. Its Consumer Sentinel database now contains at least 1,500 complaints from United Kingdom consumers against Canadian companies.[29] This increase in targeting of United Kingdom victims has prompted Project Emptor to establish an initial working relationship with the Office of Fair Trading in the United Kingdom Government. The Office of Fair Trading has also begun working regularly with the Toronto Strategic Partnership.

B. Internet Fraud

Data from the U.S. Federal Trade Commission (FTC) show that the number of fraud-related complaints of all types that consumers file with the FTC is rising significantly. Fraud-related complaints increased from 107,890 in 2000 to 133,891 in 2001 to 218,284 in 2002. Moreover, the percentages of these complaints that involve Internet-related fraud are also rising significantly. Internet-related fraud complaints have increased from 31 percent in 2000 to 42 percent in 2001 and 47 percent in 2002.[30] Similarly, in 2001 the Internet Fraud Complaint Center – a joint venture of the FBI and the National White-Collar Crime Center in the United States – received 49,711 complaints (including both fraud and non-fraud complaints, such as computer intrusions, spam/unsolicited e-mail, and child pornography) at its website and referred 16,775 complaints of fraud, the majority of which was committed over the Internet or similar online service. The total dollar loss from all IFCC-referred fraud cases in 2001 was $17.8 million, with a median dollar loss of $435 per complaint.[31]

Other FTC data show specifically that both the numbers and relative percentages of Internet-related cross-border fraud complaints have been steadily increasing in the past three years. Internet-related fraud complaints (excluding identity theft) rose from

---

[29] This total may understate the number of actual victims, because consumers may have no information about the telemarketers' actual locations or believe incorrectly that the addresses they are given are real business addresses rather than mail drops. Many Canadian telemarketers use mail drops in various border states.

[30] *See* FTC, NATIONAL/STATE TRENDS, *supra* note 3, at 3.

[31] *See* NATIONAL WHITE-COLLAR CRIME CENTER AND FEDERAL BUREAU OF INVESTIGATION, IFCC 2001 INTERNET FRAUD REPORT at 3 (2001), http://www1.ifccfbi.gov/strategy/IFCC_2001_AnnualReport.pdf.

12,213 in 2000 (representing 22 percent of cross-border fraud complaints) to 16,318 in 2001 (representing 32 percent of cross-border fraud complaints), then nearly doubled to 30,798 in 2002 (representing 34 percent of cross-border fraud complaints).[32]

C. Identity Theft

Identity theft is a comparatively new concept in the world of criminal law and law enforcement. While current criminal statutes may criminalize certain aspects of identity theft,[33] identity theft can be defined in general as any type of crime in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception, typically for economic gain. Because some authorities use the terms "identity theft" and "identity fraud" interchangeably, it may be useful to distinguish between them. Identity theft can be defined in terms of the wrongful acquisition and use of another real person's identifying data, regardless of the purpose for which the identity theft is committed,. In contrast, identity fraud can be defined in terms of the use of identifying data for the purpose of committing fraud, regardless of whether the criminal uses the user's real identity, a wholly fictitious identity, or another person's real identity.

Identity theft has become one of the fastest-growing forms of crime in Canada and the United States. In the United States, identity-theft complaints to the FTC have increased fivefold in just the last three years, from 31,117 in 2000 to 86,198 in 2001 and 161,819 in 2002.[34] In Canada, PhoneBusters received 7,629 identity-theft complaints by Canadians that reported total losses of $8,550,444.86 in 2002, and an additional 2,250 identity-theft complaints that reported total losses of $5,353,828.69 in just the first quarter of 2003.[35] At this current rate of reporting, PhoneBusters could well have 9,000

---

[32] *See* FTC, CROSS-BORDER FRAUD TRENDS, *supra* note 6, at 5.

[33] *See, e.g.*, 18 U.S.C. § 1028(a)(7).

[34] *See* FTC, NATIONAL/STATE FRAUD TRENDS, *supra* note 2, at 8.

[35] PhoneBusters data (through March 30, 2003). For earlier data including 2001 complaints, see PhoneBusters, *Statistics on Phone Fraud: Canada - Identity-Theft Complaints*, http://www.PhoneBusters.com/Eng/Statistics/idtheft_canada_stats_2001.html.

identity-theft complaints, and reported losses of more than $21 million, by the end of 2003.

One of the principal reasons for the growth of identity theft may be that -- as more and more criminals are learning – access to identifying data can be as valuable as access to physical items of value, such as cash and credit cards. As law enforcement authorities in both countries have seen, identity thieves acquire those data in many different ways to use existing accounts or open new accounts in the victims' names. The following are just a few of those ways:

- *Theft or Diversion of Mail*. By stealing consumers' outgoing mail, identity thieves can obtain many critical pieces of identifying data from the consumers' bill payments: for example, bank account numbers, Social Security and Social Insurance numbers, and credit-card numbers and expiration dates. By diverting people's incoming mail through the filing of change-of-address forms, identity thieves can intercept shipments of new checks and credit cards, "preapproved" credit-card offers in the consumers' names, and other identifying data.[36]

- *Recovery of Trash*. Some identity thieves are not reticent about rummaging through trash in order to find incoming mail or identifying data that consumers or businesses may have carelessly discarded. "Preapproved" credit-card offers, if not shredded or destroyed, can be recovered and sent back to the issuing bank by the identity thief, who can request that the card be sent to his "new" address. Even names and Social Security or Social Insurance numbers, plus address data, may be enough for an identity thief to open new accounts in the victim's name.[37]

- *"Skimming" or "Swiping" of Credit Cards*. Identity thieves, using electronic devices known as "skimmers," can "swipe" customers' credit cards at public places such as restaurants and gas stations. The skimmers record the data from the magnetic stripes on the backs of the cards. In one case, the OPP Anti-Rackets Section

---

[36] *See* June Chua, *Identity Theft – Robbery in the New Millennium*, CBC News, 2002, http://www.cbc.ca/consumers/indepth/identity/ (printed April 9, 2003).

[37] *See, e.g.*, U.S. Attorney, Western District of Louisiana, Press Release (January 18, 2002), http://www.usdoj.gov/usao/law/news/wdl20020118.html (sentence of former janitor, convicted of using another's Social Security number, who stole data from offices that he was cleaning).

investigated an organized-crime group of Russian nationals who successfully compromised the credit-card information of hundreds of customers at gas stations across the greater Toronto area. The information that had been compromised by electronically "swiping" data was transmitted to Europe where it was transferred to fraudulently manufactured credit cards. The credit cards were then used for travel or to purchase products that can be easily and quickly sold for cash to fund further criminal endeavors. This enterprise accounted for approximately CDN $1 million in losses over just three months.

- *Compromise of Government or Company Employees*. Through bribery, coercion, or other means of persuasion, government or private-sector employees with access to personal data may pass those data to outsiders for criminal use. Departments of motor vehicles or licensing, for example, may be prime targets because – in contrast to counterfeited documents – the identifying documents they issue are, by definition, "genuine" in every respect (other than the false identifying data they contain).[38] Employees with access to employee databases or consumer credit reports are also potential targets for compromise, because the identity thief can use those data to commit larger-scale crimes against multiple victims.[39]

---

[38] *See, e.g., United States v. Margot* (D. Mass., sentenced July 2002) (former Massachusetts Registry of Motor Vehicles employee provided driver's licenses in others' names to codefendant, who used them to cash counterfeit checks and obtain credit cards); *United States v. Coleman* (W.D. Wash., convicted March 2002) (defendant and coconspirators obtain identifying documents from Washington State Department of Licensing in more than 50 false identities, then used them to open bank accounts, commit bank fraud, and write worthless checks to merchants).

[39] *See, e.g.*, Ian Robertson, *Docs' IDs Used in Credit Scam*, Toronto Sun, December 13, 2002, at 22 (financial services firm worker printed customer credit profiles in connection with fraud scheme resulting in CDN $500,000 loss); U.S. Attorney's Office, Central District of California, Press Release (June 11, 2001), http://www.usdoj.gov/usao/cac/pr2001/097.html (man sentenced to 37 months imprisonment for scheme to acquire data about telephone company employees and access their online stock trading accounts); U.S. Attorney's Office, Central District of California, Press Release (January 25, 2000), http://www.usdoj.gov/usao/cac/pr/pr2000/016.htm (former temporary employee of insurance company sentenced to 27 months imprisonment for stealing private bank account data about insurance company's policyholders and using those data to

- *Theft or "Hacking" of Company Databases*. Where identity thieves cannot directly compromise company insiders, they have been known to steal government or company computers or to access computers via the Internet to obtain personal data *en masse*.[40] In the past six months, for example, a computer hard drive containing confidential data on more than 1 million people was stolen from a company in Regina, Saskatchewan,[41] and computer hard drives containing personal data on more than 562,000 U.S. active-duty and retired military and their dependents were stolen from a health care company in Phoenix, Arizona.[42]

Because identity theft can be committed without having any direct contact between the identity thief and the victim, victims may be unaware for long periods of time that someone has wrongfully used their identifying data. In 2002, a former Canadian citizen who had acquired naturalized U.S. citizenship learned that another Canadian had been misusing her Social Security number for 20 years. The victim had had her Social Security card and other identifying papers stolen in Canada in 1982. Because she had maintained her Canadian citizenship for some time thereafter, and had an aversion to applying for credit, the victim first became aware of the misuse of her number during a routine credit check incident to a purchase. In the intervening two decades, the Canadian woman who had acquired the victim's Social Security number used it to run up a credit balance of US $170,000, apply for a driver's license in Arizona, file for bankruptcy in Oklahoma, and identify herself when she was arrested.[43]

---

counterfeit 4,300 bank drafts for more than $764,000).

[40] *See, e.g.*, Allison Lawlor, *Hundreds warned as data disappears*, Toronto Globe and Mail, March 11, 2003 (reported breakin and theft of computers containing confidential personal data at provincial ministry office).

[41] *See* Steve Makris, Edmonton Journal, *Deeper threat behind computer theft*, Canada.com, February 18, 2003.

[42] *See, e.g., Massive Military Medical Info Theft*, CBSNews.com, Dec. 31, 2002, http://www.cbsnews.com/stories/2002/12/31/national/printable534819.shtml.

[43] *See* U.S. Attorney's Office, District of Arizona, Press Release (April 9, 2002) (reporting April 5, 2002 guilty plea of woman for fraudulent use of Social Security number).

A critical feature of identity theft is that it is never committed for its own sake.[44] Criminals engage in identity theft because the acquisition of other people's identifying data enables them to engage in a growing variety of other criminal acts:

- *Fraud*. Fraud is the most frequent type of crime in which identity theft plays a vital part. The FBI has reported that in its cases, fraud-related crimes in which identity theft plays a major role include bankruptcy fraud, credit-card fraud, mail fraud, and wire fraud.[45] A May 2002 "sweep" of U.S. federal criminal prosecutions for identity theft-related offenses included defendants who allegedly located houses owned by elderly citizens and assumed their identities to fraudulently sell or refinance the properties; a defendant who allegedly sold Social Security numbers on eBay; a defendant who allegedly stole the identities of 393 hospital patients to obtain credit cards using the false identities; and a defendant, already under indictment on financial crime-related charges, who allegedly murdered a homeless man and attempted to fake his own death by making it look as though the deceased victim was the defendant.[46]

- *Organized Crime and Drug Trafficking*. Law enforcement agencies have seen evidence that organized criminal groups and drug organizations commit identity theft to further their criminal enterprises. In Oregon in 2001, a series of related federal prosecutions established that a heroin/methamphetamine trafficking organization had members who entered the United States illegally and obtained

---

[44] Some hackers who obtain unauthorized access to a computer and download identifying data such as passwords or credit-card numbers may do so for personal recognition and status among other hackers, rather than for personal profit. In most other instances of identity theft, illegal gain or some other criminal purpose is the object of the crime.

[45] *See* Prepared Statement of Grant D. Ashley, Assistant Director, Criminal Investigation Division, Federal Bureau of Investigation, Before the Social Security Subcommittee of the House Ways and Means Committee (Sept. 19, 2002), http://www.fbi.gov/congress/congress02/ashley091902.htm.

[46] *See id.*; Transcript of Attorney General Remarks at Identity Theft Press Conference, U.S. Department of Justice (May 2, 2002), http://www.usdoj.gov/ag/speeches/2002/050202agidtheftranscript.htm.

Social Security numbers of other persons. The Social Security numbers that they obtained

> were then used to obtain temporary employment and identification documents in order to facilitate the distribution of heroin and methamphetamine. In obtaining employment, the defendants used false alien registration receipt cards, in addition to the fraudulently obtained SSNs, which provided employers enough documentation to complete employment verification forms. Some of the defendants also used the fraudulently obtained SSNs to obtain earned income credits on tax returns fraudulently filed with the Internal Revenue Service (IRS).[47]

- *Terrorism.* In the wake of the terrorist acts of September 11, 2001, American and Canadian government authorities have focused as never before on the mechanisms and techniques that make it possible for terrorist organizations to conduct both day-to-day activities and major destructive acts against people and property. One of the lessons learned in the past 20 months is that identity theft and fraud can play a significant role in facilitating and concealing the movements and preparatory actions of terrorists.

  In 2002, the chief of the FBI's Terrorist Financing Review Group testified that

  > terrorists have long utilized identity theft as well as Social Security Number fraud to enable them to obtain such things as cover employment and access to secure locations. These and similar means can be utilized by terrorists to obtain Driver's Licenses, and bank and credit card accounts through which terrorism financing is facilitated. Terrorists and terrorist groups require funding to perpetrate their terrorist agendas. The methods used to finance terrorism range from the highly sophisticated to the most basic. There is virtually no financing method that has not at some level

---

[47] *See* Sean B. Hoar, *Identity Theft: The Crime of the New Millennium*, 80 OR. L. REV. 1423, 1434 (2001) (footnotes omitted). As of 2001, a total of 32 defendants has been convicted in the case – 16 in federal court and 15 in state court. *Id.*

> been exploited by these groups. Identity theft is a key catalyst fueling many of these methods.
>
> For example, an Al-Qaeda terrorist cell in Spain used stolen credit cards in fictitious sales scams and for numerous other purchases for the cell. They kept purchases below amounts where identification would be presented. They also used stolen telephone and credit cards for communications back to Pakistan, Afghanistan, Lebanon, etc. Extensive use of false passports and travel documents were used to open bank accounts where money for the mujahadin movement was sent to and from countries such as Pakistan, Afghanistan, etc.[48]

The FBI official noted that when the September 11 terrorists set up dozens of bank accounts to move money to fund their activities, they made up Social Security numbers and used those numbers in filling out account applications and obtaining driver's licenses.[49] In addition, many of the terrorist cells that law enforcement authorities have been investigating use identity theft.[50]

Notwithstanding its growing importance, identity theft is not consistently treated as a serious and distinct criminal offense in all jurisdictions across Canada and the United States. The United States has a federal identity theft offense with substantial criminal penalties,[51] as well as other offenses that may be applied to certain aspects of

---

[48] Prepared Statement of Dennis M. Lormel, Chief, Terrorist Financial Review Group, Federal Bureau Of Investigation, on S. 2541, Identity Theft Penalty Enhancement Act, Before the Subcommittee on Technology, Terrorism and Government Information of the Committee on the Judiciary, United States Senate (July 9, 2002), *reprinted at* http://www.fbi.gov/congress/congress02/idtheft.htm.

[49] *See Hijackers Had 35 U.S. Bank Accounts*, CBS News.com, July 10, 2002, http://www.cbsnews.com/stories/2002/07/10/attack/main514687.shtml.

[50] *Id.*

[51] *See* 18 U.S.C. § 1028(a)(7).

identity theft.[52] Forty-eight of the 50 states have some form of laws against identity theft,[53] although not all of these statutes treat identity theft as a felony. Canada has no separate federal offense of identity theft, although the federal Criminal Code includes other offenses that may be applied to certain aspects of identity theft.[54] Recently, the Canadian Association of Chiefs of Police (CACP) have called upon the Government of Canada, through the Minister of Justice and Attorney General, to amend the federal Criminal Code to reflect the seriousness of identity theft. Specifically, the CACP recommended inclusion of (1) a section which deals with possession of multiple identities; and (2) a section that prohibits the sale or use of novelty identification documents capable of being used as a means of personal identity information.

D. Africa-Related Fraud Schemes

Solicitations by mail, fax, telephone, and e-mail that offer bogus opportunities to assist persons in Africa in laundering illegal proceeds or transferring other funds out of Africa have been a longstanding problem for law enforcement in Canada, the United States, and the United Kingdom. In the United States, the Financial Crimes Division of the Secret Service receives each day approximately 100 telephone calls from victims/potential victims and 300-500 pieces of related correspondence about such schemes.[55] United States Treasury officials reportedly have estimated that annual losses

---

[52] *See, e.g.*, 18 U.S.C. §§ 1028 (identification document fraud), 1029 (access-device fraud), 1030(a)(4) (computer fraud), 1341 (mail fraud), 1342 (use of false names in mail fraud scheme), 1343 (wire fraud), 1344 (financial institution fraud), and 1708 (theft or receipt of stolen mail matter) and 42 U.S.C. § 408 (misuse of Social Security number).

[53] *See* FTC, *ID Theft: State Laws*, http://www.consumer.gov/idtheft/statelaw.htm (viewed April 9, 2003).

[54] *See, e.g.*, C.C.C. §§ 57 (forgery of passport), 58 (fraudulent use of citizenship certificate), 345 (stopping mail), 342-342.01 (theft and forgery of credit cards), 342.1 (unauthorized use of computer), 356 (theft from mail), 366 (forgery), 368 (uttering forged document), 369 (instruments for forgery), 380 (general fraud), 381 (mail fraud), and 403 (personation with intent to commit a crime).

[55] *See* United States Secret Service, Public Awareness Advisory Regarding "4-1-9" or "Advance Fee Fraud" Schemes (2002), http://www.secretservice.gov/alert419.shtml.

to these schemes are in the hundreds of millions of dollars.[56] In Canada, the Royal Canadian Mounted Police (RCMP) reports that approximately 10,000 to 15,000 letters presenting variations of this fraud from Nigeria have circulated in Canada, and estimates that Canadians have lost approximately $30 million to these scams over the last ten years.[57] In the United Kingdom, the National Criminal Intelligence Service has reported that in 2002, 150 residents of Great Britain were known to have been defrauded by such schemes for a total of £8.4 million – an average loss of £56,675.[58]

Moreover, the explosive growth of the Internet has made it possible for organizers of these Africa-related fraud schemes to use mass e-mail solicitations (sometimes called "spam") as a means of maximizing their outreach to prospective victims at minimal marginal cost. One private-sector newsletter that tracks Internet fraud schemes calculated in 2002 that there are approximately 200 versions of these online solicitations.[59] The Secret Service has indicated that it receives tens of thousands of e-mails every month reporting Africa-related fraudulent solicitations.

Not surprisingly, these types of solicitations – designated as "foreign money offers" in FTC's Consumer Sentinel complaints – were the leading source of U.S. consumers' cross-border fraud complaints about companies in other foreign countries. In general, there were 4604 complaints in 2002 by U.S. consumers against companies in all African nations.[60] Foreign money offer complaints (58 percent) far exceeded any other category of U.S. complaints about companies in other foreign countries, such as

---

[56] *See* Brian McWilliams, *Nigerian Money Scams Thrive On The Internet*, NEWSBYTES, February 20, 2002.

[57] *See* Royal Canadian Mounted Police, *Nigerian Letter Scam* (updated February 25, 2003), http://www.rcmp-grc.gc.ca/scams/nigerian_e.htm.

[58] *See* Boris Heger & Brian Brady, *Crackdown on ££8.4m African sting*, Scotland on Sunday, March 2, 2003, http://www.scotlandonsunday.com/uk.cfm?id=258082003.

[59] *See* Stanley A. Miller II, *4-1-9 Fraud Reaches Out via E-Mail*, E-Commerce Times, March 20, 2002, http://www.newsfactor.com/perl/printer/16861/.

[60] *See* FTC, CROSS-BORDER FRAUD TRENDS, *supra* note 6, at 17. Nigeria accounted for 3,212 complaints; South Africa, 905; Togo, 267; and the Ivory Coast, 220. *See id.*

Internet auctions (14 percent) or shop-at-home/ catalog sales (8 percent).[61] In fact, 68 percent of all complaints by U.S. consumers about foreign money offers were against companies or individuals located in Africa.[62]

These totals may be inadvertently misleading in certain respects. Complaining consumers may have believed, based on information in the initial e-mails, that the persons who sent them were located in particular countries. In fact, the true senders of those e-mails – especially if they used Internet-based e-mail addresses – could have sent them from anywhere in the world. As a result, these complaints may actually involve a lone individual sending e-mail from an Internet café in Lagos or New York, or multiple people sending bulk e-mails from various sites in Africa, Europe, or North America.

---

[61] *See* FTC, CROSS-BORDER FRAUD TRENDS, *supra* note 6, at 11.

[62] *See id.* at 19.

Section II: The Response to Mass-Marketing Fraud, 1998-2003

Canadian and U.S. law enforcement agents serve a search warrant on a cross-border telemarketing fraud operation. (Source: U.S. Postal Inspection Service)

The 1997 Report contained a number of specific recommendations for collective action by the Governments of Canada and the United States against cross-border telemarketing fraud. As this Chapter will show, both countries have carried out all of those recommendations to the fullest extent possible under respective national laws and legal processes.

In the interest of brevity, the text of this Report will address only selected recommendations and their implementation. Complete status reports by Canada and the United States on their respective implementation of all recommendations will be made available on the websites of the Solicitor General and the Department of Justice, respectively.

A. Substantive and Procedural Laws

The first of the 1997 Report's recommendations was that both countries "clearly identify telemarketing fraud as a serious crime."[63] As part of their implementation of this recommendation, both countries pursued several avenues to modify existing laws and enact new laws to combat cross-border telemarketing fraud more effectively.

1. Canada

At the federal level, the Government of Canada obtained changes to the Competition Act (Bill C-20);[64] the Extradition Act and Canada Evidence Act (Bill C-40); and Omnibus *Criminal Code* Amendments (Bill C-51),[65] as well as legislation related to Proceeds of Crime, and Wiretapping which include elements that impact on telemarketing cases.[66]

---

[63] 1997 REPORT, *supra* note 7, at 7.

[64] Bill C-20, which amended the federal *Competition Act*, received Royal Assent on March 11, 1999. It introduced a new telemarketing fraud offence that can be committed in two ways: (1) "deceptive telemarketing" provisions; and (2) "failure to disclose specified information" provisions. The offence created by Bill C-20 is hybrid; it is punishable by five years imprisonment and/or an unlimited fine for the indictable offence or by a maximum of 1 year imprisonment and/or a $200, 000 fine for the summary offence (ss.52.1(9) *Competition Act*). The *Criminal Code* offence of fraud is punishable by ten years imprisonment where the value of the suspect/matter of the fraud is at least $5,000. It is punishable by two years imprisonment in other cases.

[65] The *Criminal Code of Canada* was also amended (C-51 Royal Assent on March 11, 1999) to make the telemarketing fraud an "enterprise crime" offence thereby authorizing the state to seize and forfeit proceeds of crime generated by the activity.

[66] Bill C-20 extended the *Criminal Code* wiretap provisions to authorize electronic surveillance where telemarketing offences are investigated (183 cr.) *(see s. 462.3 Criminal Code of Canada at Tab 2)*.

At the provincial level, since 1997 various statutes in Alberta and Ontario have also been passed that provide more ways to deal with telemarketing fraud.[67] In 1999, for example, Alberta enacted the Fair Trading Act, which includes specific provisions that govern loan brokers. The Act may be applied when either the business or the consumers reside in Alberta, and allows Alberta courts to use affidavit evidence when the victims reside outside the province.

2. United States

Two federal laws provide significant enhancements to existing fraud-related criminal offenses under United States federal law:

- *Senior Citizens Against Marketing Scams Act*. A federal statute (18 U.S.C. § 2326), enacted as part of the Senior Citizens Against Marketing Scams Act of 1994, directs that federal courts, in sentencing defendants for certain offenses in connection with the conduct of telemarketing, impose additional terms of imprisonment for up to five or ten years in addition to the sentence that would otherwise apply for that offense. Subsequently, the United States Sentencing Commission adopted several amendments that authorize federal judges to impose higher sentences in various situations pertinent to cross-border fraud cases. These amendments include sentencing enhancements where the offense involves "mass-marketing" (defined to include telemarketing, the Internet, or mass mailings), where a substantial part of the scheme is committed from outside the United States, or where the offense involved more than 10 victims.[68]

- *Deceptive Mail Prevention and Enforcement Act*. This Act,[69] which became effective on April 12, 2000, added new measures to protect consumers from deceptive mailings and sweepstakes. It protects consumers by establishing standards for sweepstakes mailings, skill contests and facsimile checks, as well as restricting government "look-alike" documents. Moreover, it compels every promoter to

---

[67] *See* DEPARTMENT OF THE SOLICITOR GENERAL, CANADIAN STATUS REPORT ON CANADA-UNITED STATES COOPERATION AGAINST CROSS-BORDER TELEMARKETING FRAUD (June 6, 2000), http://www.sgc.gc.ca/policing/crs_CanadianStatus_e.pdf.

[68] *See* United States Sentencing Guidelines § 2B1.1(b)(2) and (8).

[69] Public Law 106-168, Title I, 113 Stat. 1806 (1999).

establish a notification system that permits individuals to remove their names and addresses from mailing lists upon request. Marketers must maintain a record of all "stop mail" requests and be able to suppress these names for five years. The requests must be submitted in writing and can be from the individual personally or from an individual's guardian or conservator. The Act emphasizes that required disclosures must be "clearly and conspicuously displayed" and "readily noticeable, readable and understandable" by the target audience. Two specific disclosures include: no purchase is necessary to enter a sweepstakes and a purchase will not improve consumers' chances of winning a prize. The law also provides strong financial penalties for companies that do not disclose all terms and conditions of a contest. The law further provides the Postal Service the authority to issue administrative subpoenas in cases of noncompliance.[70]

In addition, in January 2003, the FTC promulgated an amended version of its Telemarketing Sales Rule ("TSR" or "Rule").[71] The TSR implements the Telemarketing and Consumer Fraud and Abuse Prevention Act, one of the U.S. federal government's main law enforcement tools against abusive telemarketing. The majority of the provisions went into effect on March 31, 2003. The FTC often charges violations of the TSR in lawsuits that it brings against telemarketers based in Canada. Among the amendments that may affect cross-border telemarketing are the following:

- Establishment of a national "Do Not Call" registry that will make it illegal for most telemarketers or sellers to call a numbers listed on the registry by a participating consumer.

- Restrictions on unauthorized billing and the purchase and sale of unencrypted consumer account numbers for telemarketing.

---

[70] To identify violations of the statute and ensure swift, appropriate investigative attention the Postal Inspection Service created the Deceptive Mail Enforcement Team. Questionable promotions identified by the team, as well as those received as consumer complaints, are examined for compliance. If possible violations are identified the information is forwarded to the appropriate field division for review and investigative attention.

[71] *See* 68 Fed. Reg. 4580 (Jan. 29, 2003); 16 CAR 310.

- Requirements that telemarketers transmit their telephone number and, if possible, their name to a consumer's caller ID service to protect consumer privacy, increase accountability on the part of telemarketer, and help in law enforcement efforts. This provision will take effect one year after the release of the Rule.

- Requirements on telemarketers to disclose the legal limits on a cardholder' s liability for unauthorized charges in the sale of credit card loss protection.

- Requirements for additional disclosures about prize promotions including the disclosure that any purchase or payment will not increase a consumer's chances of winning.

B. Task Forces and Strategic Partnerships

1. Telemarketing Fraud

a. Québec - Project COLT

The oldest of the interagency task forces established to combat telemarketing fraud in Canada is Project COLT (Center of Operations Linked to Telemarketing). Established April 1, 1998, COLT is a multiagency project based in Montreal that is staffed by the RCMP, the Sûreté du Québec (Québec Provincial Police), and the Montreal Urban Community Police, with U.S. participation by the FBI, the Bureau of Immigration and Customs Enforcement (ICE) (formerly the United States Customs Service), and the United States Postal Inspection Service.[72] Because of its focus on fraudulent telemarketing operations within the province, COLT has had three principal objectives: (1) traditional fraud investigations with multijurisdictional elements (e.g., victims located in the United States or other provinces); (2) assistance to U.S. law enforcement counterparts to facilitate extraditions in fraudulent telemarketing cases; and (3) a proactive prevention program involving private-sector companies.[73]

---

[72] *See* U.S. Customs Service, Press Release (May 2001), http://www.customs.gov/hot-new/pressrel/2001/0507-00.htm.

[73] *See* RCMP Best Practices, *Project COLT - Fraudulent Telemarketing* (Sept. 15, 1999), http://www.rcmp-learning.org/bestdocs/english/fsd/economic/colt.htm.

Since its inception, COLT has had a substantial impact on fraudulent telemarketing operations based in Québec. In 2002, for example, COLT was responsible for a total of 53 search warrant executions, 15 executions of general warrants to suspend service to telemarketers' telephones, 6 extraditions to the United States (with 20 other pending extraditions), the indictment of 24 persons in the United States and 5 persons in Canada, and the conviction of 3 persons in the United States and 3 persons in Canada (with other cases still pending).[74]

In an effort to support the ongoing efforts of Project COLT, a new task force, consisting of the Competition Bureau, the FTC, and the Postal Inspection Service has been proposed to address fraudulent and deceptive mass marketing originating in the Province of Québec. This proposed task force, which would cooperate and coordinate with the ongoing work of Project COLT, would focus on mass marketing such as scams involving lotteries, sweepstakes, toner and business supplies, directories, weight loss, health products/baldness treatments, credit repair and advance fee loans/credit cards. The Postal Inspection Service has also agreed to provide significant funding for this new task force.

b. Ontario - Toronto Strategic Partnership

In 2000, the FTC, the Toronto Police Service Fraud Squad, the Ontario Ministry of Consumer & Business Services, and the Competition Bureau of Industry Canada formed the Toronto Strategic Partnership. The purpose of the Partnership is to provide a mechanism for U.S. and Canadian law enforcement to work together in combating Toronto area-based telemarketing fraud. Other members of the Partnership include the U.S. Postal Inspection Service, the Ontario Provincial Police Anti-Rackets Section, and the Ohio Attorney General's Office. Affiliates include the York Regional Police, Barrie, Ontario Police, Royal Canadian Mounted Police, and PhoneBusters. Other agencies are also under consideration for full membership in the Partnership. In addition, the Strategic Partnership coordinates with the U.S. Department of Justice's Office of Foreign Litigation and the United States Attorney's Office for the Southern District of Illinois.

The Partnership has proved to be highly productive. In 2002, its efforts led to 66 arrests and 206 charges laid in Ontario, 31 search warrants executed, and 44 companies

---

[74] Project COLT statistics. These statistics do not reflect the fact that many of the subjects were charged with multiple offenses, primarily based upon the number of victims.

closed, as well as the indictment of 10 Canadian nationals on 51 counts of mail fraud by a federal grand jury in Harrisburg, Pennsylvania. As part of its Partnership efforts, the FTC also has sent or offered to send U.S. victims to testify in Canadian criminal proceedings in approximately twenty cases, often leading to convictions or guilty pleas. Finally, in June 2002, Strategic Partnership members released a joint consumer education brochure, "Hang Up on Cross-Border Phone Fraud." In recognition of these accomplishments, the Partnership and its members have received a number of public awards.[75]

The FBI, through Operation Canadian Eagle (see below), and the RCMP have also worked together in Ontario on a number of significant investigations involving major schemes that offered fraudulent investment opportunities.

c. British Columbia - Project Emptor

Project Emptor was established in 1998 as a dedicated telemarketing task force in British Columbia. The task force operates within the office of "E" Division, RCMP Commercial Crime Section. The task force is currently comprised of three full -time regular RCMP investigators, two investigators from the British Columbia Ministry of Public Safety and Solicitor General Compliance and Regulatory Branch, one investigator from the Competition Bureau of Industry Canada (currently vacant), one FBI Special Agent assigned from the FBI Los Angeles Field Office, and one full-time intelligence analyst/investigative assistant.

Project Emptor is project-oriented and mandated to conduct investigations of fraudulent, deceptive, or misleading telemarketing activity in the Province of British Columbia and to assist foreign law enforcement in the investigation of British Columbia -based fraudulent telemarketers (as opposed to fraudulent mail solicitation or

---

[75] The Partnership was awarded the Consumer Agency Achievement Award from the National Association of Consumer Agency Administrators for 2001, as well as the Bronze Award for Innovative Management at the IPAC (Institute of Public Administration Canada) 2002 National Conference. The participants from the Ontario Ministry of Consumer and Business Services also received the 2001 Amethyst Award for Outstanding Achievement by Ontario Public Servants for "coordinating efforts to successfully combat telemarketing and cross-border fraud, recover victims' money and bring dozens of alleged swindlers to justice."

fraudulent Internet activities). Project Emptor does not pursue Canadian *Criminal Code* charges, but uses a variety of investigative approaches, including –

- *Investigative partnerships*. Working partnerships have been established with the Federal Bureau of Investigation, United States Department of Justice, United States Postal Service, British Columbia Ministry of Public Safety and Solicitor General, the Canada Customs and Revenue Agency, Canada Post, Industry Canada Competition Bureau, Office of Fair Trading (United Kingdom), courier companies, telephone companies and the banking industry to identify fraudulent telemarketing activity. These agencies make extensive use of PhoneBusters National Call Centre and the United States- based Consumer Sentinel databases for identification of suspects and victims.

- *Federal criminal prosecution in the United States*. During 2002, 13 Canadian citizens were indicted in the United States relating to Project Emptor investigations: 12 were indicted by federal grand juries and one charged by criminal complaint. To date, all criminal prosecutions in the United States relating to Project Emptor have been prosecuted by the United States Attorney's Office in Los Angeles, California. Since 1999, that office has brought 16 criminal prosecutions against 37 individuals operating telemarketing schemes from British Columbia and Québec.[76] A number of these cases have involved requests for assistance under the *Mutual Legal Assistance Treaty* (MLAT) along with the *Extradition Act*. More than a dozen Canadian citizens are pending extradition to the United States in relation to fraudulent telemarketing investigations. As a result of these prosecutions, 5 Canadian citizens are currently serving or have served lengthy jail sentences in the United States relating to Project Emptor investigations, with sentences ranging from 2.5 years to 10 years in custody.

- *The British Columbia Trade Practice Act*. Through civil actions under the *Trade Practices Act* of British Columbia, Project Emptor has seized or restrained approximately CA $33 million worth of assets from fraudulent telemarketing operations in British Columbia. Seizures have included bank accounts, cash, properties, luxury import vehicles and offshore racing boats. Seizures are liquidated and proceeds returned to victims primarily in the Unites States. As of

[76] Summaries of these prosecutions and other cross-border enforcement actions may be found in the Appendix.

December 2002, civil actions had been brought against 48 individuals and 13 corporate entities using approximately 200 different company names.

- *Federal civil actions in the United States*. The FTC has brought 8 civil actions against British Columbia - based telemarketers under the provisions of section 5 of the Federal Trade Commission Act, which prohibits unfair and deceptive acts and practices in interstate and foreign commerce. These cases have yielded millions of dollars in consumer redress, against individuals and companies operating telemarketing schemes from British Columbia.

d. FBI - Operation Canadian Eagle

Since 1999, the FBI has conducted "Operation Canadian Eagle." Canadian Eagle is an FBI operation in which agents from three designated field offices are assigned to work on temporary duty in Canada with specific Canadian law enforcement agencies to investigate fraudulent cross-border telemarketing. Agents from the FBI's Boston field office have worked with Project COLT in Montreal, agents from the FBI's Detroit office have worked with RCMP representatives in Ontario, and agents from the FBI's Los Angeles field office have worked with Project Emptor.

e. Other Approaches

In addition to these formal task forces and partnerships, individual agencies are making greater use of their existing civil and administrative authority to combat cross-border fraud schemes. In the area of lottery schemes, the Postal Inspection Service has obtained tentative and final orders that mandate the respondent to cease and desist from conducting any scheme for the distribution of money or property by lottery, and that instruct postmasters to send this detained mail for return to sender, marked "LOTTERY MAIL." The Postal Inspection Service also works in conjunction with ICE to identify, intercept and destroy foreign lottery mail before it enters the United States. Suspected foreign lottery mail is turned over to the Postal Inspection Service for a determination of nonmailability. Once a determination is made, then a destruction order is issued for destruction of the mail. In FY 2002, approximately 849,000 pieces of foreign lottery mail were destroyed prior to entering the mailstream. Since the initiative began in 1994, approximately 4.6 million pieces have been destroyed.

2. Africa-Related Fraudulent Schemes

The vast expansion of fraudulent schemes with ostensible connections to Africa has made it necessary for law enforcement authorities in North America to work more closely with government authorities in Africa in combating these schemes. Coordination measures have included the following:

- *Stationing of Investigators in Other Countries*. The United States Secret Service has established an office in Lagos, Nigeria to enable its agents to work more closely with Nigerian authorities.

- *Interception of Bulk Mail*. On April 29, 1998, a Memorandum of Understanding was signed between the United States Postal Service and the Nigerian Postal Service to prevent U.S. citizens from being victimized in these schemes. The agreement allows the Postal Service to remove such letters from the mailstream and destroy them once it is determined they bear counterfeit Nigerian postage stamps or meter impressions. Since April 1998, Postal Inspectors have removed and destroyed more than 5 million fraudulent 4-1-9 letters. During FY 2002, Postal Inspectors in New York seized and destroyed over 27,000 such letters. In the six months prior to the seizures, Inspectors received approximately 90,000 inquiries or complaints related to 4-1-9 letters in its automated fraud database; in FY 2002, Inspectors received only 15,484 inquiries or complaints there. While this tactic has been effective in reducing the number of 419 letters via the U.S. mail, scheme operators have increasingly shifted to sending their fraudulent solicitations via fax and e-mail.

C. Consumer Reporting and Information-Sharing Systems

The 1997 Report identified the use of "hotlines" as a promising practice that could assist law enforcement and the public. Both countries have not only implemented the "hotline" concept for fraud complaints, but have greatly expanded the hotline approach to encompass online reporting of fraud.

1. Canada

Canada has been taking three significant steps to improve the receipt and use of fraud complaints by the public: (1) the expansion of PhoneBusters beyond its original mandate of telemarketing fraud; (2) the establishment of Project RECOL (Reporting of

Economic Crime On-Line); and (3) the creation of Canshare, a web-based database connecting consumer affairs departments across Canada.

- *PhoneBusters*. PhoneBusters was originally established in 1993 as a joint forces initiative, with a mandate to identify, investigate, and seek prosecution of illegal telemarketers from Montreal who were preying on residents of Ontario and other parts of Canada. Over time, the complaints received at PhoneBusters grew to include not only telemarketing fraud, but also frauds by mail, fax, and the Internet. From 1995 to the present, PhoneBusters received complaints from 15,000 Canadian victims of telemarketing fraud totalling CDN $51.9 CDN million losses. From 1996 to the present, PhoneBusters also received complaints from 15,200 American victims reporting losses of US $91.1 million.

  By 1997, PhoneBusters evolved from an investigative unit to a fraud intake complaint centre and crime prevention and investigative support unit. In 2001, the OPP and the RCMP entered into a Memorandum of Understanding creating the PhoneBusters National Call Centre (PNCC). The PNCC is the only police led call centre and consists of OPP, RCMP and more that 60 community volunteers. The PNCC plays an important role in combating telemarketing fraud by educating the public and collecting and disseminating victim evidence to the appropriate enforcement agencies. The PNCC crime prevention program has caused a decrease in the number of Canadian and Ontario residents who fall victim to criminal telemarketers in Ontario. Because these telemarketers continue to target primarily residents of the United States and other countries, PhoneBusters receives complaint data on a national level and seeks to analyze and disseminate it to dedicated enforcement units.

- *RECOL*. To meet the growing need for a national mechanism for online reporting of criminal activity, the RCMP established Project RECOL (Reporting Economic Crime Online). RECOL, which is expected to come online during 2003, will receive and analyze complaint data and determine how best to refer information to appropriate investigative units.

- *Canshare*. In November 1998, Canshare was officially launched at a meeting of federal, provincial, and territorial ministers responsible for consumer affairs in Canada. Canshare is intended to facilitate information-sharing among law enforcement and consumer agencies, such as consumer complaints, and to provide a mechanism for early warning alert notices to consumer protection and

law enforcement agencies.[77] In 2002, Canshare was incorporating data from Ontario, Alberta, Saskatchewan, the Federal Competition Bureau, and PhoneBusters, and most jurisdictions were posting alerts.[78] Canshare is now exploring whether U.S. law enforcement agencies can be provided access to its resources as well.

2. United States

In addition to the national toll-free numbers that the FTC maintains for fraud-related complaints (1-877-FTC-HELP/1-877-382-4357) and identity-theft related complaints (1-877-IDTHEFT/1-877 -438-4338), the United States now has two major resources for consumer complaints relating to mass-marketing fraud. These are Consumer Sentinel and the Internet Fraud Complaint Center.

a. Consumer Sentinel

Established in November 1997, Consumer Sentinel is a secure, law enforcement website developed by the FTC, in cooperation with its law enforcement partners,[79] through which member agencies have immediate and secure access to consumer complaints and make them and other investigative information about consumer fraud and deception available to law enforcement.[80] Consumer Sentinel currently has approximately 750,000 Internet, telemarketing, and other consumer fraud-related complaints provided by numerous public and private entities. During 2002, Consumer

---

[77] *See* Canadian Intergovernmental Conference Secretariat, Press Release (Nov. 13, 1998), http://www.scics.gc.ca/cinfo98/83063514_e.html.

[78] *See* INTERNAL TRADE SECRETARIAT, AGREEMENT ON INTERNAL TRADE, CHAPTER EIGHT – CONSUMER - RELATED MEASURES AND STANDARDS: ANNUAL REPORT TO THE AIT SECRETARIAT at 4 (March 24, 2002), http://www.intrasec.mb.ca/pdf/chpt8_e.pdf.

[79] Consumer Sentinel, which the FTC maintains, is a joint project whose leading partners include the National Association of Attorneys General (NAAG), the U.S. Postal Inspection Service, the National Consumers League, PhoneBusters, the U.S. Secret Service and the Australian Competition and Consumer Commission.

[80] *See* Federal Trade Commission, *Consumer Sentinel*, http://www.consumer.gov/sentinel.

Sentinel received more than 200,000 fraud-related complaints about transactions involving more than $343 million.[81] More than 100 organizations contribute data to Consumer Sentinel, including numerous local Better Business Bureaus, the Internet Fraud Complaint Center, the National Fraud Information Center, Xerox, PhoneBusters, and the Social Security Administration Office of the Inspector General.

The collected investigative information in Consumer Sentinel is accessible to federal, state, and local law enforcement agencies in the United States, Canada, and Australia through a secure, password-protected website. Approximately 670 Canadian and U.S. agencies have access to the database. Users can search the Sentinel database using any of 22 fields alone or in combination.

A special feature of Consumer Sentinel for United States Armed Forces is Military Sentinel. Established in September 2002, Military Sentinel is a project of the FTC and the Department of Defense to identify and target consumer protection issues that affect members of the United States Armed Forces and their families. Military Sentinel also provides a gateway to consumer education materials covering a wide range of consumer protection issues, such as auto leasing, identity theft, and work-at-home scams. Members of the United States Armed Forces are able to enter complaints directly into Consumer Sentinel. Through Consumer Sentinel, the government password-protected Website, this information can be used by law enforcement agencies, members of the JAG staff, and others in the Department of Defense to help protect armed services members and their families from consumer protection-related problems.[82]

The Consumer Sentinel network also supports a multinational project to gather and share cross-border e-commerce complaints, econsumer.gov. Recognizing that the growth of e-commerce has made cross-border fraud and consumer confidence in e-commerce matters of multinational concern, in April 2001 the FTC and 12 other members of the International Consumer Protection and Enforcement Network (ICPEN) (formerly called the International Marketing Supervision Network) established Econsumer.gov. Today, 17 countries and the Organisation for Economic Cooperation and Development participate in this project. Econsumer.gov has a multilingual public website that provides (in English, French, German, and Spanish) general information

---

[81] *See* FTC, CROSS-BORDER FRAUD TRENDS, *supra* note 6, at 2.

[82] *See id.* at 3.

about consumer protection in all countries that belong to the ICPEN, contact information for consumer protection authorities in those countries, and an online complaint form.[83] Using the existing Consumer Sentinel network, the incoming complaints will be shared through the government website with participating civil and criminal consumer protection law enforcers.[84]

Pursuant to the Identity Theft and Assumption Deterrence Act of 1998, the FTC has also established the Identity Theft Data Clearinghouse. Launched in November 1999, the Data Clearinghouse is the sole national repository of consumer complaints about identity theft. The Clearinghouse provides specific investigative material for law enforcement and larger, trend-based information providing insight to both the private and public sectors on ways to reduce the incidence of identity theft. Information in the Clearinghouse is available to law enforcement members via Consumer Sentinel, the secured, password-protected government website. This access enables law enforcers to readily and easily spot identity theft problems in their own backyards, and to coordinate with other law enforcement officers where the data reveal common schemes or perpetrators.[85]

b. Internet Fraud Complaint Center

Established in May 2000, the Internet Fraud Complaint Center (IFCC) is a joint project of the FBI and the National White Collar Crime Center. The IFCC's mission is to address criminal fraud committed over the Internet. For victims of Internet fraud, IFCC provides a convenient and easy-to-use online reporting mechanism that alerts authorities to suspected violations. For law enforcement and regulatory agencies at all levels, IFCC offers a central repository for complaints related to Internet fraud, works to quantify fraud patterns, and provides timely statistical data of current fraud trends.[86]

---

[83] *See* http://www.econsumer.gov.

[84] *See* FTC, CROSS-BORDER FRAUD TRENDS, *supra* note 6, at 4.

[85] *See id.*

[86] *See* FBI and National White Collar Crime Center, *Internet Fraud Complaint Center*, http://www1.ifccfbi.gov/index.asp.

In 2001, the IFCC website received a total of 49,711 complaints (including fraud and non-fraud complaints, such as computer intrusions, SPAM/unsolicited email, and child pornography), and referred 16,775 complaints of fraud, the majority of which was committed over the Internet or similar online service. The total dollar loss from all referred cases of fraud was $17.8 million, with a median dollar loss of $435 per complaint.[87] From complaints in 2001, agencies that voluntarily provided information reported 1867 investigations initiated from complaints, 3 arrests derived from complaints, $51,427.63 in documented restitution to the victims, and 26 victims who had their complaints handled through refunds, receipt of ordered merchandise, or resolved through other agreed-upon arrangements.[88] In addition, the IFCC provided vital support for the FBI's Operation Cyber Loss (see below).

In 2002, the IFCC website received 75,063 complaints (including fraud and non-fraud complaints), and the IFCC referred 48,252 complaints of fraud – a three-fold increase from the previous year. The total dollar loss from all referred cases of fraud was $54 million, up from $17 million in 2001, with a median dollar loss of $299 per complaint.[89] In response to the September 11, 2001 terrorist attacks in New York and Washington, D.C., the IFCC devoted a substantial quantity of its resources after September 11 to receiving and processing terrorism-related information from the public, while continuing to make referrals on non-terrorism issues. IFCC referrals were directly responsible for several successful federal and state criminal prosecutions in 2002.[90]

---

[87] *See* NATIONAL WHITE COLLAR CRIME CENTER AND FBI, IFCC 2001 INTERNET FRAUD REPORT at 3 (2002), http://www1.ifccfbi.gov/strategy/IFCC_2001_AnnualReport.pdf.

[88] *See id.* at 18.

[89] *See* NATIONAL WHITE COLLAR CRIME CENTER AND FBI, IFCC 2002 INTERNET FRAUD REPORT at 3 (2002), http://www1.ifccfbi.gov/strategy/2002_IFCCReport.pdf.

[90] *See id.* at 13-15.

D. Enforcement Accomplishments

Both Canadian and American prosecutors and civil enforcement attorneys have successfully litigated against numerous criminals and their businesses for cross-border fraud schemes. The following list sets forth just a few examples of these criminal and civil cases.[91]

1. Telemarketing Fraud

- *United States v. Levine* (D. Mass., arrested February 2001). In February 2001, members of Project COLT arrested a U.S. citizen (Mark Levine) in connection with an investigation of a Montreal-based telemarketing operation. Levine, who was wanted in North Carolina in connection with another telemarketing fraud-related case, ultimately was sentenced to 57 months imprisonment in North Carolina. On September 16, 2002, Levine was sentenced to 75 months imprisonment in Boston – to run consecutively to the 57-month sentence previously imposed – and restitution of $1.3 million. As a result, Levine will be required, under federal sentencing guidelines, to serve 11 years imprisonment (less "good time" credit).[92]

- *United States v. Impellezzere* (D. Ariz., arrested June 7, 2001). In 2001, Angelo Impellezzere, a resident of Quebec, traveled to an assisted living facility to meet with an 84-year-old telemarketing fraud victim. Impellezzere posed as an undercover Canadian police officer, using an alias, and told the victim, who had already lost $80,000 to criminal telemarketers, that he needed another $10,000 from her so that her funds could be traced back to the people who had defrauded her of the $80,000. He was arrested when he arrived after midnight at the victim's assisted-living facility, to pick up not only her $10,000 but another $7,500 that he had persuaded another victim to wire to her so that he could pick up the funds at the same time. On November 26, 2001, Impellezzere pleaded guilty to one count of money laundering in the United States District Court in connection

---

[91] More detailed summaries of these and other cross-border fraud prosecutions and enforcement actions can be found in the Appendix.

[92] *See* Royal Canadian Mounted Police in Quebec, News Release (September 24, 2002).

with the alleged scheme. On February 20, 2002, Impellezzere was sentenced to 21 months imprisonment.

- *FTC v. Windermere Big Win Int'l,* 1:98cv08066 (N.D. Ill., filed Dec. 16, 1998, final order issued Aug. 17, 2000). In 1998, the FTC filed a civil complaint against 5 individual and 3 corporate defendants who induced elderly consumers to buy shares in a Canadian lottery ticket or series of tickets at prices ranging from $39 to almost $600. The FTC charged that the telemarketers violated the FTC Act and the Telemarketing Sales Rule by falsely claiming that it was legal to buy and sell foreign lottery tickets, failing to disclose to consumers that the sale of, and trafficking in foreign lotteries is a crime in the United States, and making other false statements to induce consumers to buy the tickets. The U.S. district court issued a permanent injunction prohibiting deceptive claims and ordering $19.7 million in restitution to victims. The U.S. Department of Justice's Office of Foreign Litigation filed a parallel civil action in Canada, and was able to have the restitutionary provisions of the U.S. district court's judgment enforced by the Ontario Superior Court of Justice and affirmed by the Court of Appeal.[93]

- *Regina v. Nichols* (Ontario Super. Ct., sentenced 1998). As part of his fraudulent activities, an Ontario telemarketer who purported to sell packages of lottery tickets, Reed Nichols, had persuaded an 84-year-old woman living in Chicago to give him $1,005,000. On April 8, 1999, a judge in Toronto, Ontario sentenced Nichols to 5 years and three months' service in the penitentiary. In his opinion, the judge made clear that he would have sentenced Nichols to a seven-year term of imprisonment had Nichols not returned the balance of the funds, approximately $772,000, to the victim.

- *United States v. Cartagena*, No. CR 00-613 (C.D. Cal., indictment filed June 8, 2000). In 2000, Eduardo Cartagena had managed lottery boiler rooms in Burnaby, British Columbia, that were part of an operation called, at various times, Global Dividends International, Horizon 2000 Investments International, and Platinum International. The day after Cartagena's arrest in the United States on May 9, 2000, RCMP officers, in cooperation with the British Columbia Ministry of the Attorney General and the FBI, conducted searches at two telemarketing boiler rooms in Burnaby. At trial, Cartagena was convicted on 10 counts of wire fraud.

---

[93] *See United States v. Ernest Levy et al.*, [2002] O.J. No. 2298 (Ontario Sup. Ct. Justice – C. Campbell J.) (affirmed by the Court of Appeal - 10 January 2003).

The testimony at trial showed that the business name was changed often to avoid detection of the scheme. On May 14, 2001, Cartagena was sentenced to 70 months imprisonment and restitution to victims.

- *Regina v. American Family Publishers, Publishers Central, and First Canadian Publishers and Sharma* (Quebec Super. Ct., pleaded guilty March 5, 1999). This criminal case, brought by the Competition Bureau of Industry Canada in Quebec, charged corporate entities operating under the names American Family Publishers, Publishers Central, and First Canadian Publishers, and the company's president, Vijay Sharma, with violating the misleading advertising provisions of the Competition Act. On March 5, 1999, the defendants pleaded guilty to the charges. On May 5, 1999, the Quebec Superior Court imposed a $1 million fine against the corporate entities, and a $100,000 fine against Sharma. The sentence was the highest ever imposed against a deceptive telemarketing operation under these provisions of the Act. Previously, on March 11, 1999, the Court sentenced four other telemarketers to jail terms ranging from two to six months and 20 to 120 hours of community service. One additional telemarketer who pleaded guilty was fined $5,000, and a second additional telemarketer who pleaded guilty was to be sentenced in June 1999.[94]

2. Internet Fraud

- *United States v. Kallmann*, No. 03-CR-00635IEG (S.D. Cal., pleaded guilty March 11, 2003). As a result of the October 2001 anthrax incidents, Charles W. Kallmann, now the former chief executive officer of 37Point9, Inc., exploited the publicity from these incidents to fraudulently promote the sale of his company's stock by issuing false press releases promoting a purported anti-anthrax product. The press releases (some of which were posted on the Internet) made various false and misleading claims about the product. Around the time that the false press releases were issued, the volume of trading in 37Point9 shares increased approximately 1,500 percent to more than 32 million shares and the price increased approximately 300 percent. Canadian and American investors bought 37Point9 stock as a result of the fraudulent conduct. On March 11, 2003,

---

[94] *See* Competition Bureau, Press Release (May 5, 1999), http://strategis.ic.gc.ca/SSG/ct01521e.html.

Kallmann pleaded guilty in a criminal information to two counts of securities fraud.[95]

- *Regina v. Friskie* (Saskatchewan Provincial Court, charges laid 2000)/*FTC v. Skybiz.com, Inc. et al.*, Civil Action No. 01-CV-0396-EA (N.D. Okla., complaint filed May 30, 2001). In 2000 and 2001, law enforcement and regulatory agencies around the world, including Canada and the United States, brought a series of related criminal and civil actions against SkyBiz.com. Skybiz purported to sell online tutorials on Web-based products, using website presentations, in-person sales presentations, seminars, teleconferences, and other marketing material, to tout the opportunity to earn thousands of dollars a week by recruiting new "Associates" into the program.[96] Authorities, however, charged that SkyBiz was an illegal pyramid scheme. In May 2000, a SkyBiz associate, Jeanette Friskie, was charged in Saskatchewan with operating a pyramid scheme.[97] On September 24, 2001, the Provincial Court of Saskatchewan determined that SkyBiz was a pyramid scheme, found Friskie guilty of running an Internet-based pyramid scheme, and fined her CA $20,000.[98]

  In a related civil proceeding, in May 2001, the FTC filed a civil action in U.S. District Court in Tulsa, Oklahoma, against six individuals and four corporations including SkyBiz.com. The FTC charged that the SkyBiz.com scheme may have defrauded consumers of approximately $175,000,000 worldwide. At the request of the FTC, the District Court halted all unlawful activities of the SkyBiz operation, froze the defendants' assets to preserve them for consumer redress,

---

[95] *See* Criminal Division, United States Department of Justice, Press Release (March 11, 2003), http://www.usdoj.gov:80/opa/pr/2003/March/03_crm_149.htm.

[96] *See* FTC, Press Release (June 18, 2001), http://www.ftc.gov/opa/2001/06/sky.htm.

[97] *See* Lori Enos, EcommerceTimes.com, *U.S. Files Charges over $175M Online Pyramid Scheme*, NewsFactor.com, June 19, 2001, http://www.newsfactor.com/perl/story/11346.html.

[98] *See* R. v. Friskie, [2001] S.J. No. 565, Information No. 24021184 (Saskatchewan Provincial Court, Sept. 24, 2001); Law Society of Saskatchewan, News Archives 2001, http://www.lawsociety.sk.ca/newlook/archive/Archive01Dec.htm.

appointed a receiver,[99] and later ordered the return of assets, including tens of millions in an account in Ireland, to the United States, for possible use as consumer redress. (Distribution of this redress fund will begin in the near future.) Ultimately, in January 2003, the FTC reached a settlement with nine of the ten defendants shortly before trial that would provide US $20 million for consumer redress. The settlement also barred all of the defendants from participating in pyramid schemes or misrepresenting the amount of sales, income, profits or rewards of any future business venture. The tenth defendant also settled with the FTC shortly before trial.[100] The FTC received substantial assistance from the RCMP and other international consumer protection law enforcement bodies, including the Australian Competition and Consumer Commission, the South African Department of Trade and Industry, the New Zealand Commerce Commission, and the United Kingdom Department of Trade and Industry.

3. Identity Theft

- *Regina v. Taft* (B.C. Super. Ct., pleaded guilty June 7, 2002). Between November 1998 and August 2000, an American citizen who remained illegally in Canada (Anthony B. Taft) obtained personal information from individuals by running advertisements in the "Help Wanted" sections of local newspapers and inducing respondents to provide copies of identification papers. Taft then forged or applied for identification in the names of the victims, opened bank accounts under their names, and deposited counterfeit checks in the accounts and withdrew funds. Over a two and one-half month period, Taft obtained almost $80,000 CA in cash by cashing counterfeit checks and making withdrawals. In Québec, Taft, using the name of one of his victims, also ran a website for making false identification documents. Police later found among Taft's personal materials both American and Canadian passports of real people; Taft was able to insert his photograph onto the passports so that he could travel at will under other victims' names. On June 7, 2002, after spending 12 months in pretrial custody, Taft pleaded guilty to 23 fraud-related offenses. On June 26, 2002, Taft

---

[99] *See* FTC, Press Release (June 18, 2001), http://www.ftc.gov/opa/2001/06/sky.htm.

[100] *See* FTC, Press Release (March 24, 2003; corrected Apr. 1, 2003), http://www.ftc.gov/opa/2003/03/skybiz.htm.

was sentenced to a total of three months, after the sentencing judge determined that the sentence, coupled with his pretrial detention, was the equivalent of a 27-month sentence. On February 11, 2003, the British Columbia Court of Appeal sentence upheld the sentence.

D. Public Education and Prevention Accomplishments

Since 1997, Canadian and American law enforcement authorities have shown great creativity in developing and participating in a wide range of public education and prevention measures that involve cross-border fraud.

1. Reverse Boiler Rooms

In its discussion of public education and prevention measures, the 1997 Report cited as a promising practice the use of "reverse boiler rooms": i.e., projects in which senior volunteers and law enforcement representatives contact telemarketing fraud victims and provide information about how to avoid victimization in the future.[101] Both countries have not only continued, but substantially expanded on, this approach.

In Canada, since 1997 PhoneBusters has also been host to Seniorbusters. Seniorbusters is a community-based initiative in which senior volunteers -- through telephone contact, educational materials, and speaking engagements – educate other seniors on how to avoid becoming victims of telemarketing fraud.[102] From October 15, 1997 through May 31, 2001, Seniorbusters volunteers gave 9,220 hours of their time and reached 2,101 Canadian victims and 980 U.S. victims.[103]

In the United States, after 1997 the AARP conducted a number of reverse boiler rooms in cities throughout the United States. In Philadelphia, for example, an AARP-sponsored reverse boiler room, "Operation Freedom Rings," that took place on July 23,

---

[101] *See* 1997 REPORT, *supra* note 7, at 24.

[102] Department of the Solicitor General, Press Release, *Solicitor General Andy Scott Renews Funding for Seniorbusters Telemarketing Fraud Prevention* (June 29, 1998), http://www.sgc.gc.ca/publications/news/19980629_e.asp.

[103] *See* PhoneBusters, *Seniorbusters*, http://www.PhoneBusters.com/Eng/Statistics/sb_data.html (accessed April 9, 2003).

1998, made 7,581 telephone calls and spoke to 3,152 people.[104] One of the people called was about to send a $3,000 check to a fraudulent scheme.[105] The FBI Los Angeles Division also has operated, on a weekly basis, a reverse boiler room similar to PhoneBusters, in which seniors contact other people whose names appear on "mooch lists" or "sucker lists."[106]

2. Interception and Return of Victim Proceeds

In the last several years, Project COLT, the Ontario Strategic Partnership, and Project Emptor have been made it a part of their anti-telemarketing fraud duties to intercept checks and money orders that victims have sent to Canadian telemarketing schemes and return those check and money orders to the victims. At Project Emptor, the intercepted funds have been returned to U.S. victims with assistance provided by the Federal Bureau of Investigation. At Project COLT, the intercepted funds are now being returned directly to U.S. victims by ICE agents. ICE agents personally visit a victim and explain how telemarketing fraud works; in appropriate circumstances, they may also seek assistance form and or public social services.

This approach has resulted in the return of millions of dollars to telemarketing fraud victims. As shown below in Table 6, Project COLT, from 1998 to 2002, has returned a total of more than US $11.5 million.

---

[104] *See* Letter from Anita O'Riordan, AARP, to Jonathan Rusch, U.S. Department of Justice (August 21, 1998).

[105] *See* Alliance Against Fraud in Telemarketing and Electronic Commerce, *Member News*, FOCUS ON FRAUD, Fall 1998, at 4.

[106] *See* Alliance Against Fraud in Telemarketing and Electronic Commerce, *Enforcement Action*, FOCUS ON FRAUD, Fall 1998, at 2. The AARP has since concluded its operation of reverse boiler rooms.

Table 6 - Project COLT Statistics on Return of Victim Funds, 1998-2002			
Year	**Victims Reporting to COLT**	**Losses Reported to COLT**	**Funds Returned by COLT**
1998	1,143	$14,385,938	$5,102,106
1999	1,089	$7,175,612	$1,259,436
2000	1,759	$15,972,730	$2,492,066
2001	5,641	$25,653,587	$1,691,906
2002	2,823	$19,251,333	$1.020.890
Total	**12,455**	**$82,439,200**	**$11,566,404**

The Toronto Strategic Partnership and Project Emptor have also returned substantial funds to victims. Since February 2000, law enforcement authorities working in Ontario have seized more than CA $1.1 million for return to consumers, including $119,282.95 in 2002. In 2002, Project Emptor returned more than US $450,000 to victims.

3. Public Advisories

In the past several years, both Canada and the United States have made increasing use of public advisories to warn the public about specific types of fraud. In the wake of the terrorist attacks on September 11, 2001, both the United States Department of Justice and the RCMP separately issued public advisories about telemarketing and Internet fraud schemes that falsely claimed to be seeking donations on behalf of the victims of those attacks.[107] The FTC also held press conferences and issued a press alert to deter fraudulent charitable fund-raising schemes related to the

[107] *See* U.S. Department of Justice, *Special Report on Possible Fraud Schemes - Solicitations of Donations for Victims of Terrorist Attacks* (updated September 27, 2001), http://www.usdoj.gov/criminal/fraud/WTCPent-SpecRpt.htm; RCMP News Release, *Phone and Internet solicitations requesting donation* (September 26, 2001) (updated November 21, 2002), http://www.rcmp-grc.gc.ca/news/2001/nr-01-24.htm.

tragedy and issued public alerts and warnings to deal with other disaster-related scams such as the marketing of bogus bioterrorism products on the Internet.[108]

More recently, at the 2002 Cross-Border Crime Forum, the Canadian Department of the Solicitor General and the United States Department of Justice jointly issued a public advisory about Africa-related fraudulent e-mail solicitations.[109] In addition, PhoneBusters frequently issues public advisories on fraud issues, such as international fax/mail schemes emanating from Spain.[110]

One technique that agencies in both countries have also used successfully to educate the public about certain Internet frauds is the creation of so-called "mock" or "teaser" websites. These websites are designed to appear initially to the public as though they are offering the types of goods, services, or investment opportunities that fraudulent operations generally offer (e.g., "high-yield" investments). After the consumer clicks through two or three pages within the site, however, he or she comes to a page that provides a warning and information about that type of online scheme. At

---

[108] *See* Federal Trade Commission, Consumer Alert, *Helping Victims of the Terrorist Attacks - Your Guide to Giving Wisely* (issued Sept. 2001), available at http://www.ftc.gov/bcp/conline/pubs/alerts/victimalrt.htm; Consumer Alert, *Offers to Treat Biological Threats: What You Need to Know* (issued Oct. 2001 in cooperation with the Centers for Disease Control and Prevention and the Food and Drug Administration), available at http://www.ftc.gov/bcp/conline/pubs/alerts/bioalrt.htm; Press Release, FTC Cracks Down on Marketers of Bogus Bioterrorism Products: Agency Tells Web Operators Get Off the Net or Face Prosecution (issued Nov. 19, 2001), available at http://www.ftc.gov/opa/2001/11/webwarn.htm; FTC Broadens Warnings to Marketers of Bioterrorism Defense Products: E-mails Focus on Questionable Claims for Bioterrorism Protection Devices (issued Jan. 2, 2002), available at http://www.ftc.gov/opa/2002/01/round2web.htm.

[109] *See* Department of the Solicitor General and U.S. Department of Justice, Public Advisory: Special Report on Africa-Related E-Mail Solicitations (July 22, 2002), http://www.usdoj.gov/criminal/SpecRptR.pdf.

[110] *See* RCMP, Press Release, *PhoneBusters Issues Caution On International Fax/Mail Prize Scams*, Jan. 22, 2003, http://www.rcmp-grc.gc.ca/news/nr-03-01.htm.

various times, the Ontario Ministry of Consumer and Business Services, the FTC, and the U.S. Securities and Exchange Commission have set up such sites.

In the area of identity theft, several agencies have taken different but complementary approaches to using websites for public education and prevention. The FTC, the Privacy Commissioner of Canada, and the Ontario Ministry of Consumer and Business Services maintain identity theft websites that include extensive information on how identity theft is committed and guidance on what to do if someone becomes an identity theft victim.[111] The U.S. Department of Justice maintains a website on identity theft that includes public information about criminal investigations and prosecutions, and a quiz for consumers that can be used by law enforcement and consumer groups in public presentations.[112]

4. Public Service Announcements and Campaigns

Both Canada and the United States have launched significant public service advertising campaigns to warn the public about various frauds. In Canada, the RCMP, in partnership with the Ontario Provincial Police (OPP) and the Department of the Solicitor General, developed two new sets of public-service announcements (PSAs), in English and French, about three of the most prevalent telemarketing schemes: West African letter fraud, lottery fraud, and identity theft. These 30-second PSAs were distributed to all Canadian television media beginning May 15, 2002.[113]

---

[111] *See* FTC, *Identity Theft*, http://www.consumer.gov/idtheft; Ontario Ministry of Consumer and Business Services, *ID Theft Online (Winter 2002)*, http://www.cbs.gov.on.ca/mcbs/english/55XMY3.htm; Privacy Commissioner of Canada, *Identity Theft: What it is and what you can do about it*, http://www.privcom.gc.ca/fs-fi/02_05_d_10_e.asp.

[112] *See* U.S. Department of Justice, *Identity Theft: A Quiz for Consumers*, http://www.usdoj.gov/criminal/fraud/idquiz.pdf.

[113] *See* RCMP, Media Advisory: "PhoneBusters" PSA helps public avoid telemarketing scams (May 15, 2002), http://www.rcmp-grc.gc.ca/news/2002/nr-02-08.htm.

In addition, the Deceptive Telemarketing Prevention Forum[114] spearheaded a $300,000 national public education/prevention program that was conducted through a private and public sector partnership. In the spring of 1998, Forum members adopted the campaign slogan, "Stop Phone Fraud - It's a Trap!," and began developing and implementing a social marketing strategy to fight deceptive telemarketing. As part of that strategy, federal, provincial and territorial Ministers responsible for consumer affairs, through the Consumer Measures Committee, provided financial support and unveiled a poster and pamphlet which provide basic information on how to detect and report phone fraud. Subsequently, under the leadership of the Forum, the PhoneBusters website was upgraded, and public service announcements and an education video were released.

In the United States, both the U.S. Postal Inspection Service and the FTC have been highly active in devising public-service campaigns that involve cross-border fraud. In August 2002, for example, the Postal Inspection Service sponsored a campaign known as "National Fraud Against Senior Citizens Awareness Week," in close cooperation with the FTC and the Senior Action Coalition of Pittsburgh, Pennsylvania. The campaign was specifically developed to do two things: (1) to educate consumers – not only senior citizens but their families and caregivers – about the signs of fraudulent activities that target seniors and how to report them to the appropriate authorities; and (2) to increase the public's awareness of the enormous impact that fraud has on senior

---

[114] The Forum consists of members from government, the private sector and not-for-profit organizations, which include: Visa Canada, MasterCard, Bell Canada, Stentor, the Canadian Association of Retired Persons, the Canadian Marketing Association, PhoneBusters (Ontario Provincial Police), the RCMP, the Canadian Bankers Association, Canada Post, the Solicitor General of Canada, the National Consumer Measures Committee, the Canadian Council of Better Business Bureaus, and the Volunteer Centre of Toronto. The Competition Bureau of Industry Canada acts as Forum Chair. The Forum's terms of reference are (1) to gather and share intelligence in the area of deceptive telemarketing; (2) to discuss and formulate measures that members and other stakeholders may implement in combating deceptive telemarketing; and (3) to inform and educate the general public concerning telephone fraud practices to reduce the number of potential victims. *See* PhoneBusters, Deceptive Telemarketing Forum, http://www.PhoneBusters.com/Eng/DeceptiveTelemarketingForum/index.html.

citizens. The basic message of the campaign was: "Take the time to reach our seniors. Or someone else will."[115]

---

[115] This campaign began with a Senate Resolution, introduced by Senators Carl Levin (MI) and Susan Collins (ME), which was passed on June 27, 2002, designating the week of August 25, 2002, as "National Fraud Against Senior Citizens Awareness Week." The campaign then used a multi-media approach to get the message to as many people as possible. This approach included:

- Appearances by actress Betty White, the national spokesperson for the campaign, in public service announcements (PSAs) and video messages. Televised PSAs began airing on August 25, 2002, and reached an audience of more than 1.9 million. Radio PSAs reached an audience of more than 47 million, and the satellite media tour reached an audience of more than 4 million.
- A Video News Release (VNR) produced by the Postal Inspection Service for use during our national and local media events, which included an introduction by Betty White, a 15-second and a 30-second PSA, and a two-minute segment featuring Attorney General John Ashcroft together with the Solicitor General of Canada.
- A national press conference held at U.S. Postal Service Headquarters in Washington, DC, on August 26, 2002, announcing the initiative. Chief Postal Inspector Lee Heath, Postmaster General John Potter, and FTC Chairman Timothy Muris participated in the conference.
- An August 26, 2002, press conference held by the Postal Inspection Service's Northeast Division in Maine, at which Senator Susan Collins was the keynote speaker.
- An August 27, 2002, press conference hosted by the Postal Inspection Service's Western Allegheny Division in Pittsburgh.
- Posters, placed in 38,000 post office lobbies across the country, which prominently displayed the prevention message and included the FTC's toll-free telephone number and the U.S. Postal Inspection Service Web site address (www.usps.com/postalinspectors) so that consumers could gather additional information and/or report suspected fraudulent activity.
- Half-page newspaper advertisements (with the same visual and text message as the poster) placed in 36 selected newspaper markets with circulation to over 13.8 million readers.
- Distribution of approximately 3 million mail pieces (with the same visual and text message as the poster) to select ZIP codes with concentrations of senior households that were anticipated to reach approximately 1.5 million seniors.

The FTC has developed an array of brochures, pamphlets, and webpages on various types of consumer frauds, including cross-border fraud. Its brochures now include titles such as "Border-Line Scams Are The Real Thing," "Custom-ized Cons Calling," "Foreign Lotteries: The Games You Can''t Win," "Going Shopping? Go Global! A Guide for E-Consumers," "International Lottery Scams," "The 'Nigerian' Scam: Costly Compassion," and "Hang Up On Cross-Border Phone Fraud." In the case of the latter brochure, the FTC published it with five other members of the Toronto Strategic Partnership.[116] More recently, it has been developing plans for a set of video PSAs on identity theft.

- Production by North American Precis Syndicate (NAPS) of a series of three print articles covering senior fraud topics. Distribution of the articles included metropolitan newspapers, community daily newspapers, and community weekly newspapers. A minimum of 10,000 newspapers were contacted beginning the week of August 25, 2002, and every two weeks thereafter for a three-month-period.
- Approximately 300,000 statement inserts (with the same visual and text message as the poster) were distributed along with consumers' stamp orders by the U.S. Postal Service's Stamps by Mail fulfillment center in Kansas City from September through November 2002.

While it would be impossible to determine the number of consumers the campaign touched, during just the first week of the campaign the FTC received 1,129 telephone calls from consumers as a result of the campaign.

[116] The FTC's partners in this consumer education effort included Canada's Competition Bureau, the Ontario Ministry of Consumer and Business Services, the Ontario Provincial Police Anti-Rackets Investigation Bureau, the Toronto Police Service, and the U.S. Postal Inspection Service. The brochure, available in English and French, provides tips for distinguishing between legitimate telemarketing and fraudulent schemes. It specifically warns consumers about phony prize promotions, foreign lottery schemes, advance-fee loan rip-offs, travel offer scams, unnecessary credit card loss protection, and identity theft, and provides a central contact point in each country to report telemarketing complaints.

This brochure and the FTC's publications are available on the FTC's cross-border fraud website, http://www.ftc.gov/bcp/conline/edcams/crossborder/index.html. This website, which the FTC unveiled in December 2002, contains information about cross-border scams for consumers and businesses, and links to law enforcement information.

The Postal Inspection Service also plans to launch an Identity Theft Awareness campaign in 2003. This campaign will have many of the same aspects as the National Fraud Against Senior Citizens Awareness Week campaign, including (1) posters highlighting ID theft prevention tips and a contact number for consumers to call to obtain additional information and/or report concerns; (2) a major mailing providing ID theft prevention tips; (3) PSAs; (4) a new/updated video on ID theft; (5) ID theft prevention and victim action tips posted on numerous Web sites; and (6) newspaper ads and published articles on ID theft.

5. Public-Private Sector Partnerships

Government and private-sector organizations in both countries have likewise expanded their public education and prevention measures on major frauds like telemarketing fraud. For example, in Canada, the "Stop Phone Fraud - It's a Trap" marketing campaign, as described above, provided public- and private-sector entities with a variety of educational materials and resources. In the United States, the National Consumers League, with a grant from the United States Department of Justice, developed a "Telemarketing Fraud Education Kit" for distribution to government agencies, nonprofit consumer, civic, community, and labor organizations, and schools.[117]

Recently, on February 19-20, 2003, the FTC held a two-day public workshop on public-private partnerships against cross-border fraud.[118] This workshop brought together, speakers, panelists, and audience members from government agencies, the business sector, and consumer groups across the United States and Canada to discuss how the public and private sectors could work together more effectively to combat various types of cross-border fraud. The workshop was organized into panels that focused on the role of a variety of private sector groups -- including financial institutions, credit card companies, ACH processors, money transmitters, commercial mail receiving agencies, courier services, industry associations, Internet Service

---

[117] *See* Alliance Against Fraud in Telemarketing and Electronic Commerce, *Resources*, FOCUS ON FRAUD, Spring 2002, at 4. The Kit includes tips on common telemarketing schemes and how to avoid them; scripts for oral presentations, and PowerPoint presentations, to various audiences; brochures about telemarketing fraud against seniors; and advice on conducting effective consumer education. *Id.*

[118] *See* Federal Trade Commission, *Partnerships Against Cross-Border Fraud* (February 25, 2003), http://www.ftc.gov/bcp/workshops/crossborder/index.html.

Providers, and Internet domain registrars -- in combating cross-border fraud. The workshop generated several proposals for the private and public sectors to work together to identify, stop, and bring effective enforcement actions against cross-border fraud operators and ideas for other measures that the private sector can take to assist law enforcement in combating cross-border fraud.

Section III: Current Challenges in Cross-Border Fraud - Towards A Binational Action Plan

Now this is not the end. It is not even the beginning of the end. But it is, perhaps, the end of the beginning. - Winston Churchill

Since 1997, Canada and the United States have made greater strides than ever in binational cooperation to combat cross-border fraud. As the preceding Section indicated, joint task forces have been established; new laws and procedures have been established; a number of major investigations into significant cross-border fraud schemes have been conducted; a number of criminal prosecutions and civil enforcement actions against major fraud schemes have been brought in both countries; and in some cases, a number of significant custodial sentences and financial penalties have been imposed. All of these developments are not only welcome; they have been necessary elements of a broader strategy to combat major cross-border schemes effectively.

Yet Canadian and American law enforcement's efforts against cross-border fraud are far from done. The substantial growth in the number of telemarketing operations across North America, the incursion of organized crime into telemarketing fraud, the continuing expansion of identity theft in North America and elsewhere – these are but a few of the reasons that law enforcement still has much to do before it reaches "the beginning of the end" in combating cross-border fraud.

Nonetheless, Canadian and American law enforcement have reached "the end of the beginning." In general, investigators, prosecutors, and civil enforcers in both countries are better informed than ever about the nature of major fraud schemes, and better equipped with a variety of legal tools to root out these schemes and bring their organizers, operators, and key subordinates to justice. Now that both countries have effectively accomplished all of the recommendations in the 1997 Report, law enforcers, prosecutors, and regulators in both countries should 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 those steps, this Report presents an Action Plan that outlines key measures to strengthen existing binational capabilities to combat the most significant types of cross-border fraud that affect both countries. This Action

Plan addresses strategic and operational concerns regarding investigation, prosecution, and public education and prevention of cross-border fraud schemes.

A Binational Action Plan for Cross-Border Fraud

The Action Plan consists of 12 points grouped under five principal headings:

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.***

After 1997, both countries at the national level tended to operate independently in formulating, discussing, and deciding on their respective national strategies for combating cross-border telemarketing fraud. Once these basic strategies were set, law enforcement representatives in both countries have frequently conferred and closely cooperated with each other on specific task forces, projects, and cases. In light of more recent developments in criminal telemarketers' methods of operations, it would be highly appropriate for national-level working groups in both countries to discuss their current strategic frameworks in greater detail and to identify any areas where greater harmonization of those strategies may be in order.

❑ ***(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.***

In November 2001, the Binational Working Group on Cross-Border Telemarketing Fraud received approval to expand its mandate to all types of cross-border mass-marketing fraud, including Internet fraud. More recently, concerns in Canada about the dramatic growth of identity theft led to establishment of a National Identity Theft Working Group, now a subgroup of Canada's National Mass Marketing Fraud Strategy Group. This Subgroup has recently participated by videoconference in meetings of its United States counterpart, the Identity Theft Subcommittee of the Attorney General's Council on White Collar Crime. As authorities on Canada move forward in formulating their response to identity theft, it may be appropriate to have continued coordination between these two bodies about national strategies and

measures. In addition, both countries should consider whether they have other working groups on fraud issues with cross-border implications, such as Internet fraud and Africa-related fraud schemes, that would benefit from consultation and information-sharing efforts.

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.***

Each of the ongoing task forces, strategic partnerships, and operations that have been active in Canada – Project COLT, Project Emptor, Operation Canadian Eagle, and the Toronto Strategic Partnership – have demonstrated their worth through concrete results. Each has had significant accomplishments in rooting out and taking enforcement action against major fraud schemes. All of them need to continue their work, and to build on their accomplishments and find ways of having even greater impact on criminal telemarketing operations in their respective areas.

In 2003, the FBI received approval from the United States Department of Justice for continued funding of Operation Canadian Eagle. This development is welcome because it helps to ensure continuity in the numerous investigations that it has been supporting. It is important that all participating agencies reaffirm their commitment to the task forces and strategic partnerships, even as national security and counterterrorism concerns are placing extraordinary stresses on law enforcement throughout North America. In addition, where other agencies may have investigative or information resources that could prove useful, task forces and strategic partnerships should consider inviting those other agencies to become participants as well. Because all law enforcement agencies must operate under various resource constraints, agencies need to ensure that personality differences or "turf-consciousness" do not stand in the way of effective collective action against major fraud schemes.

❑ ***(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 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.***

Tracing of the proceeds of major cross-border fraud schemes can be a daunting task for even experienced investigators and prosecutors. Organizers and leaders of telemarketing fraud and Internet fraud schemes often take great pains to conceal and disguise the channels through which they launder the proceeds of their crimes. Nonetheless – as the task forces and strategic partnerships in Canada have seen – tracing, seizing, and forfeiting the proceeds of such frauds offer two substantial benefits. First, demonstrating that law enforcement can literally "take the profit out of crime" sends an important message to criminals who are considering whether to begin or continue fraudulent operations. Second, returning the maximum possible amounts to victims of the frauds is not only an appropriate means of reducing the long-term harm to those victims, but in some jurisdictions may be required of prosecutors and judges as part of the sentencing process.[119] Law enforcement and prosecutive agencies should therefore incorporate consideration of seizure and forfeiture into their strategic planning of particular cases, and use all available legal authority as appropriate in those cases.

In this regard, one promising practice, which deserves wider attention among prosecutors in both countries, is the use of procedures under mutual legal assistance arrangements to effect freezes of bank accounts in Canada. Canadian law now provides that when a United States court has issued a restraining order in connection with a criminal prosecution, a Canadian court may enter an order enforcing that restraining

---

[119] In federal criminal prosecutions that involve telemarketing fraud, a federal statute, 18 U.S.C. § 2327, specifically directs that when a defendant is convicted of any of seven offenses – identification-document or identity theft (18 U.S.C. § 1028), access-device or credit-card fraud (18 U.S.C. § 1029), mail fraud (18 U.S.C. § 1341), use of fictitious name or address in mail fraud (18 U.S.C. § 1342), wire fraud (18 U.S.C. § 1343), financial institution fraud (18 U.S.C. § 1344), or conspiracy to commit any of those offenses (18 U.S.C. § 371) – in connection with the conduct of telemarketing, the sentencing court will "order restitution to all victims of any [such] offense . . . ." 18 U.S.C. § 2327(a). Section 2327 makes the issuance of that order mandatory, regardless of the defendant's economic circumstances or the fact that a victim has received, or is entitled to receive, "compensation for his injuries from the proceeds of insurance or any other source." *Id.* § 2327(a), (b)(4)(A) and (B). The order must direct the defendant to pay to the victim (through appropriate court mechanisms) "the full amount of the victim's losses" (i.e., all losses that the victim suffered as a proximate result of the offense). *Id.* § 2327(b)(1) and (3).

order. This approach has been used successfully in several Project COLT cases.[120] Canadian and United States prosecutive authorities should disseminate detailed information about these procedures to prosecutors' offices for potential use in future cross-border fraud 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.***

The 1997 Report highlighted continuing concerns about the efficiency of the process for obtaining formal assistance under the Mutual Legal Assistance Treaty (MLAT). It urged both countries to clarify the circumstances where formal MLAT requests are in fact needed, by providing information and advice to agencies involved.[121] Prosecutors and investigators in both countries continue, at various times, to decry what they perceive to be the lack of speed in processing MLAT requests. There is no doubt that, in the aftermath of the September 11 terrorist attacks, counterterrorism and national security interests have placed a vastly greater burden on the bilateral MLAT process and the law enforcement professionals who implement that process.

Even so, it would be beneficial for both countries to review recent MLAT requests in fraud cases and to develop a list of best (and "worst") practices for prosecutors to consult in preparing and submitting such requests. Broader dissemination of exemplary documents needed for MLAT requests, and of guidance about the MLAT process, could also serve to make the process more efficient.

In addition to sharing information under MLATs in appropriate circumstances, agencies should continue to expand other efforts to assist each other's investigations, especially where agencies with civil authority, such as the FTC, are unable to use the (criminal) MLAT mechanism to cooperate with agencies that have either civil or

---

[120] *See, e.g.*, Homologation d'une Ordonnance de Blocage, In re Une Demande d'Entraide Présentée Par Les Etats-Unis d'Amerique Dans Le Cadre d'Une Procédure Visant Le Blocage de Certains Biens Situés Au Canada en Vertu de La Loi Sur L'Entraide Juridique en Matière Criminelle, No. 500 36-002804-022 (Montréal Cour Supérieure, May 27, 2002).

[121] *See* 1997 REPORT, *supra* note 7, at 20.

criminal authority (or both). For example, the FTC and the Competition Bureau have adopted a protocol for sharing consumer complaints and investigation information to make pursuit of cross-border fraud operators faster, more efficient, and more effective. This protocol is streamlining and enhancing cooperation under prior agreements -- particularly a 1995 agreement under which the governments of the United States and Canada agreed to use their best efforts to cooperate in the detection of deceptive marketing practices; to inform each other of investigations and proceedings involving cross-border deceptive marketing practices; to share information relating to enforcement; and, in appropriate cases, to coordinate enforcement.[122]

While both the FTC and the Competition Bureau are subject to certain confidentiality protections that restrict their ability to share investigative information, the information-sharing protocol instructs staff of both agencies to keep in regular contact to maximize the amount of information sharing and cooperation compatible with these protections. The types of information to be shared include information in the public record and, subject to confidentiality protections, consumer complaint information and consumer interview reports, information provided by anonymous informants, and opinions of expert witnesses. In certain circumstances other information will also be shared. Moreover, under a prior confidentiality agreement, the Competition Bureau has access to the more than 750,000 fraud complaints in the FTC's Consumer Sentinel database, which include Canadian complaints provided to the FTC by PhoneBusters.

❑ ***(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.***

In the last decade, federal and state prosecutors in the United States have used "sweeps" – announcements that a series of criminal cases of the same type have been brought in coordinated fashion in multiple jurisdictions – against various types of fraudulent schemes:

---

[122] The new protocol, which was developed in a series of meetings in 2002, is not a single document. Rather, it includes a joint work plan stressing increased communication and setting information sharing and cooperation priorities; guidance to staff on what information can be shared under applicable law and rules; and a template that each agency is using for information requests.

- *Telemarketing Fraud*. Federal and state prosecutors have participated in nationwide sweeps in Operation Senior Sentinel (1995) and Operation Double Barrel (1998).[123] In June 2002, the FTC, together with civil and criminal law enforcement agencies from both sides of the border, announced a series of coordinated civil and criminal law enforcement activities against Canadian telemarketers.[124]
- *Internet Fraud*. In May 2001, the United States Department of Justice and the FBI announced "Operation Cyber Loss," in which criminal charges were brought against approximately 90 individuals and companies as part of a nationwide series of investigations into Internet fraud that were initiated by the Internet Fraud Complaint Center (IFCC). The fraud schemes exposed as part of Operation Cyber Loss represented more than 56,000 victims who suffered cumulative losses of more than $117 million.[125]
- *Identity Theft*. On May 2, 2002, United States Attorney General John Ashcroft announced a "sweep" of federal criminal prosecutions relating to identity theft. In that sweep, United States Attorney's Offices in 24 judicial districts bought 73 prosecutions against 135 individuals. The crimes charged in these prosecutions ranged from fraud schemes – some of which targeted seniors, hospital patients, and corporate officers – to murder.[126]

---

[123] *See* Federal Bureau of Investigation, *Criminal Fraud Cases*, http://www.fbi.gov:80/hq/cid/fc/ec/cases/criminalecu.htm; United States Department of Justice, Press Release (December 17, 1998), http://www.usdoj.gov:80/opa/pr/1998/December/596cr.htm; United States Department of Justice, Press Release (December 7, 1995), http://www.usdoj.gov:80/opa/pr/Pre_96/December95/609.txt.html.

[124] *See* Federal Trade Commission, Press Release, *U.S., Canadian Law Enforcers Target Cross-Border Telemarketers; Scam Operations Caught in the Cross-Hairs* (issued June 10, 2002), available at http://www.ftc.gov/opa/2002/06/crossborder.htm.

[125] *See* FBI, Press Release, *Internet Fraud Investigation "Operation Cyber Loss"* (May 23, 2001), http://www.fbi.gov/pressrel/pressrel01/ifcc052301.htm.

[126] *See* U.S. Department of Justice, *Transcript of Attorney General Remarks at Identity Theft Press Conference Held With FTC Trade Commission Chairman Timothy J. Muris and Senator Dianne Feinstein* (May 2, 2002), http://www.usdoj.gov/ag/speeches/2002/050202agidtheftranscript.htm.

Criminal and civil enforcement agencies in Canada and the United States have conducted enforcement sweeps on a number of occasions. Although enforcement sweeps require close coordination among multiple jurisdictions, they have two substantial advantages over the bringing of individual fraud cases. First, they help to heighten the enforcement impact on major types of fraud, by showing that enforcement authorities can effectively work together to investigate and pursue fraud schemes. Second, they serve to call greater attention by the media, the business community, and the public to particularly egregious frauds and to educate the public about the dangers of the particular fraud schemes that have been exposed.

As circumstances permit, prosecutors and other enforcement officials in both countries in the future may want to consider organizing and conducting one or more enforcement sweeps on certain types of cross-border fraud schemes, 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.***

The 1997 Report recommended that both countries explore the use of remote testimony in criminal proceedings, by videoteleconferencing or similar means, to reduce costs.[127] Both countries have taken certain steps in this regard. Bill C-40, which received Royal Assent on June 17, 1999, amended the *Criminal Code* and the *Canada Evidence Act* to provide for the use of video-link testimony in criminal trials and extradition hearings. Canadian prosecutors have used this authority in several cases to obtain testimony from victim-witnesses in the United States.

Experience has also shown, however, that some of the concerns reflected in the 1997 Report – such as the logistical and financial considerations that can arise when witnesses must remain more than one day at a video site to give or complete their testimony – have some foundation. Law enforcement and prosecutive agencies in both countries should therefore confer about ways of effectively addressing these problems and making the process of arranging for videolink testimony from multiple locations easier. As part of this process, agencies may have to assess, on a case-by-case basis,

---

[127] 1997 REPORT, *supra* note 7, at 15.

whether it would be less costly to arrange for transportation of the victim to the venue of the criminal proceedings or to arrange for videolink testimony.

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.***

One of the perennial problems in antifraud programs (both enforcement and public education and prevention) is that basic public information about what government is doing to combat criminal fraud schemes often gets only limited attention. Because of the need to ensure fair trials and to protect the rights of the accused, press releases about particular investigations and prosecutions often limit how much information they disclose, and the press and the public typically pay little if any attention to these press releases after they are issued.

But press releases and similar mechanisms, like government websites dedicated to fraud, can serve two important functions. First, they provide important documentation of the efforts that governments are taking to protect their citizens. Consumers and businesspeople alike need to know that government agencies care about their plight when they become victims of fraud. Second, they often contain information about the schemes' methods of operations and the impact of the schemes on victims. Such information can be of great value to the investigators, prosecutors, and judges who deal with major cross-border fraud cases.

For these reasons, both countries should establish procedures to ensure that as public information is made available -- through press releases, website, or other mechanisms – about particular enforcement actions that authorities have taken against cross-border fraud schemes, that information is promptly disseminated among agency participants on all task forces, strategic partnerships, and operations that deal with cross-border fraud, and to headquarters components of those agencies.

❑ ***(9) Both countries should coordinate their efforts to contact other countries whose citizens are being targeted 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.

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.

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.***

There is strong evidence, as discussed above, that cross-border fraud schemes have strongly moved towards electronic payment mechanisms as a preferred method of obtaining victims' funds. Accordingly, governments should make it a priority to discuss the problem with key entities in the financial services and electronic payments industries. These discussions should focus on exploring possible measures that could be taken, whether individually or collectively, to reduce the use of electronic payments mechanisms by people involved in cross-border fraud schemes.

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.***

Interagency task forces routinely develop highly detailed information about the organizers and operations of fraud schemes in their respective areas. Sharing of information between these task forces, however, can be sporadic and dependent largely on happenstance, as investigators need to confer with each other on specific files. Increasing the opportunities for investigators and prosecutors to learn from each other about significant trends and issues that arise in various jurisdictions can be highly beneficial to all.

On some occasions, training on mass-marketing fraud subjects may be done on a local or regional basis. For example, in 2000 and 2001, the FTC has worked with provincial authorities in Ontario and Alberta, respectively, to conduct joint training sessions for law enforcement personnel on investigating Internet crimes. Similarly, in 2002 and 2003, the FTC, the United States Secret Service, the United States Postal Inspection Service, the International Association of Chiefs of Police, and the United States Department of Justice have jointly sponsored and conducted a series of regional training seminars on identity theft throughout the United States. These types of regional training courses are highly valuable in disseminating basic investigative techniques and concepts to various law enforcement agencies. At the same time, they are less suitable for fostering information-sharing about national fraud trends and cases and developing relationships with agencies across multiple jurisdictions.

National conferences are a more suitable mechanism for accomplishing this latter objective. In April 2002, Alberta Justice held an Economic Crime Summit in Banff, Alberta that drew more than 80 police, law enforcement agents, and prosecutors from across Canada and the United States. In January 2003, the RCMP held an Integrated Policing Workshop in North Bay, Ontario that was comparably well-attended from both countries. Authorities in both countries should ensure that there is at least one binational conference each year that can provide this kind of cross-border fraud training and information-sharing.

Other government authorities involved with the criminal justice system, including investigators, prosecutors, and judges, also hold periodic conferences on a regional or national basis. Both countries therefore should also seek to identify training seminars and conferences where oral or written presentations about various types of cross-border fraud may be appropriate, and to make speakers available for such opportunities.

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

Even with the best of intentions, travel costs, work schedules, and court calendars place serious constraints on police, law enforcement agents, and prosecutors who could benefit from training seminars and conferences held outside their immediate areas. One way of overcoming these constraints is to take advantage of videoconferencing facilities that are increasingly available in law enforcement, prosecutive, and regulatory agencies.

In January 2003, the Office of Legal Education of the United States Department of Justice and the United Kingdom Crown Prosecution Service organized and conducted a four-hour joint training conference on Internet fraud by videoconference. This joint videoconference training – the first of its kind by the Department of Justice – proved highly successful in enabling prosecutors from both countries to share information about current Internet fraud schemes, useful online investigative resources, national criminal laws applicable to such schemes, and commentary about legal and practical considerations in preparing and trying Internet fraud prosecutions.

Moreover, in February 2003, the FTC coordinated a two-hour joint training conference on cross-border health fraud by videoconference with law enforcers from both Canada and Mexico. Through this technology, dozens of law enforcers from six government agencies participated in an unprecedented videoconference linking 18 locations across the United States, Canada, and Mexico. Panelists from the FTC and the Food and Drug Administration discussed their approaches to investigating and preparing health fraud cases and answered questions posed by the participants. Canadian officials from the Competition Bureau and Health Canada connected directly from their offices in 13 cities while 20 Mexican government officials from Profeco and COFEPRIS participated through a hook-up at the U.S. Embassy in Mexico City.

The success of these videoconference sessions strongly suggests that authorities in Canada and the United States should confer about whether particular fraud-related topics -- identity theft, Internet fraud, or seizure and forfeiture of assets in fraud cases, among other possibilities – would be suitable for similar videoconference training.

* * *

Each of these measures, taken separately, offers some definite benefits for law enforcement and the public in both countries. In combination, they provide a substantial foundation for binational cooperation that can substantially reduce the scope and severity of cross-border mass-marketing fraud.

Appendix

Selected Cross-Border Mass-Marketing Fraud Enforcement Actions

The following list sets forth selected summaries of various criminal prosecutions and civil enforcement actions involving cross-border mass-marketing fraud that were undertaken in the United States and Canada during the period January 1998 - March 2003. This does not purport to be an exhaustive list of all such actions. In instances where the summaries do not report the outcome of particular arrests or charges, it is important to note that all criminal suspects or defendants are presumed innocent until found guilty in a court of law.

2003

- Criminal Prosecutions - Telemarketing Fraud

  - *Competition Bureau Case*

    On February 20, 2003, the Competition Bureau announced that charges were laid against seven individuals engaged in an Ontario-based telemarketing operation targeting U.S. residents, primarily seniors. The accused allegedly conducted promotions of a medical discount plan, using the names MedPlan, Global and STF Group (see below), induced victims to release personal banking information and then made unauthorized withdrawals from bank accounts. Consumers reportedly lost an estimated US $8 million in one year.

  - *United States v. Iyhab El-Jabsheh, et al.*, No. CR 03-217 (C.D. Cal., indictment filed March 5, 2003)

    This criminal case, brought by the United States Attorney's Office in Los Angeles, charges six defendants (Iyhab El-Jabsheh, Clifford Edwards, Darren Danbrook, William Dixon, Stephen Sean Laidlaw, and Colin Tylor) with various fraud-related charges pertaining to an alleged lottery scheme. An extradition request will be filed with Canada.

- *Regina v. Levy (Ontario)*

  This criminal case **c**harged two individual defendants, Ernest Levy and Alan Silverstein, and two corporations with unlawfully selling lottery tickets and printing information concerning betting on Ontario Lottery products, contrary to the Criminal Code. All defendants were convicted of the two sets of offenses. Each individual defendant was fined CA $50,000.

  - Press Release (Ontario Provincial Police/PhoneBusters): http://www.PhoneBusters.com/Eng/Charges_Arrests/March_17_2003.html

- Criminal Prosecutions - Internet Fraud

  - *United States v. Kallmann* (S.D. Cal., pleaded guilty March 11, 2003)

    This criminal case, brought by the Fraud Section of the Criminal Division of the United States Department of Justice, charged the former Chief Executive Officer of 37Point9, Inc., Charles W. Kallmann, with two counts of securities fraud for issuing false press releases in an effort to bolster his company's sagging stock price during the anthrax scare in 2001. 37Point9 was a thinly traded over-the-counter "penny stock." According to the criminal information, Kallmann exploited the publicity generated by the October 2001 anthrax incidents to fraudulently promote the sale of 37Point9 shares through the issuance of false press releases promoting an anti-anthrax product. In October 2001, Kallmann drafted two press releases which made false and misleading claims about the development, testing and effectiveness of a product named "SurfaceShield" which was purportedly designed to have a long term killing effectiveness against anthrax, as well as a wide variety of bacteria, viruses, germs and fungi. One of the press releases stated that a wholly owned subsidiary of 37Point9 had entered into an agreement with a laboratory "to develop an addition to its SurfaceShield product that will enable the enhanced SurfaceShield to kill bacillus anthracis (anthrax) while it is in its vegetative state and prior to release and sporulation of vegetative cells." In fact, 37Point9 had not entered into such an agreement.

Around the time of the issuance of the false press releases, the volume of trading in 37Point9 shares increased approximately 1500 percent to over 32 million shares and the price of 37Point9 shares increased approximately 300 percent. On March 11, 2003, Kallmann pleaded guilty to a criminal information charging him with two counts of securities fraud.

- Press Release (Guilty Plea): http://www.usdoj.gov:80/opa/pr/2003/March/03_crm_149.htm

- Civil and Administrative Enforcement Actions - Telemarketing Fraud

  - *FTC v. Assail, Inc. et al.*, Civ. A. No. W03CA007 (W.D. Tex., civil complaint filed Jan. 9, 2003).

    In this civil action, the FTC filed charges against seven corporations and nine individuals, the Assail Telemarketing Network, for engaging in deceptive and unfair activities in the marketing of advance-fee credit card packages under the names Advantage Capital, Capital First, and Premier One in violation of the FTC Act, the Telemarketing Sales Rule, and the Gramm-Leach-Bliley Act. In its complaint, the FTC alleges that the defendants operate an advance-fee credit card scam through a network of boiler rooms, Canadian front men, and outsourced fulfillment and customer service centers in the United States, Canada, India, and Caribbean countries. According to the FTC, the scam targets people with poor credit histories, offering credit cards that never materialize, while upselling various benefit packages through an incomprehensible, computer-generated "verification" tape. On January 9, 2003, a U.S. district court temporarily halted the defendants' operation, froze their assets, and appointed a receiver to take over the corporate defendants.

    - Press Release (Complaint): http://www.ftc.gov/opa/2003/01/assailnetwork.htm

- *FTC v. STF Group Inc. et al. [Med Plan]*, No. 02 C 0977 (N.D. Ill., civil complaint filed Feb. 10, 2003); State v. MedPlan (Mich. and R.I., civil actions filed 2002) [Toronto Strategic Partnership]

  In this civil action, the FTC charged several related companies and individuals who operated an enterprise based in Ontario, Canada that charged U.S. consumers' credit cards and debited their bank accounts without authorization with violations of the FTC Act and the Telemarketing Sales Rule. According to the FTC's complaint, the defendants allegedly initially sold worthless credit card loss protection services to consumers throughout the United States, charging them approximately $249 for their credit card protection service. In 2001, according to FTC allegations, the defendants switched to promoting a healthcare discount plan that consisted of an annual membership and a "benefit card" that purportedly entitled purchasers to substantial discounts. The defendants allegedly sold the health plan to U.S. consumers, primarily the elderly, under the names Med Plan and, later, Global Discount. The defendants allegedly told consumers at the outset that their offer was only available to consumers with a valid checking account, and asked consumers to read back their account number from a check to prove that they had a checking account. In most instances, the FTC alleges that the defendants immediately charged consumers' accounts for $349 allegedly even when consumers told the defendants that they had no interest in making a purchase. The defendants allegedly told other consumers that they would have a "trial period" of up to 35 days before the defendants charged the card. The defendants also allegedly told consumers that they could receive refunds if they were not satisfied. The FTC alleges that the defendants immediately billed most or all consumers, and consumers obtained refunds only when they complained to a law enforcement agency or the Better Business Bureau.

  A U.S. district court has entered an injunction and frozen the assets of defendants. The FTC developed this case in conjunction with the Canadian Competition Bureau, which has arrested several of the main defendants in this action. The Toronto Strategic Partnership also provided assistance to the FTC.

In another civil action, the Michigan and Rhode Island Attorneys General filed suits against MedPlan, Inc., of Toronto, Canada. The suits allege that MedPlan telemarketers called consumers, often seniors, and falsely told them they would send materials about the "MedPlan plan" - a membership club providing discounts on chiropractic, vision, and dental services, prescriptions, and other health-related services and products for $349. According to Attorneys General Granholm and Whitehouse, MedPlan telemarketers requested consumers' bank account numbers for "verification purposes" and failed to clearly disclose that the information would be used to withdraw the membership fees from consumers' accounts. Lastly, when consumers cancelled the plan, MedPlan failed to provide timely refunds to consumers. The suits seek penalties and restitution.

In a separate civil action, the Missouri Attorney General obtained a temporary restraining order against MedPlan, Inc.,prohibiting MedPlan and its employees from obtaining Missourians' bank account numbers through telemarketing calls or from making unauthorized withdrawals from consumers' accounts. The lawsuit seeks a permanent injunction, restitution, and civil penalties.

- Press Release (FTC Complaint): http://www.ftc.gov/opa/2003/02/medplan.htm
- Press Release (Michigan Civil Action): http://www.houselaw.net/houselaw/november2002/ss-mi02.html

- Civil and Administrative Enforcement Actions - Internet Fraud

- *FTC v. CSCT, Inc.*, Civil Action No. 03 C 00880 (N.D. Ill., civil complaint filed Feb. 6, 2003) (Toronto Strategic Partnership)

  This civil action, brought by the FTC in Chicago in coordination with officials in Canada and Mexico, charges four defendants – CSCT, Inc., a British Columbia-based company; CSCT, Ltd., a British company based in London, England; and their officers, John Leslie Armstrong and Michael John Reynolds -- with making false claims that CSCT can treat cancer by using an electromagnetic device to kill cancer cells. The FTC alleges that the company uses its Internet website to advertise this treatment to

consumers in the United States and elsewhere. According to the FTC, the defendants charge consumers $15,000 up front for several weeks of "treatments" with the electromagnetic device. Consumers must travel at their own expense to Tijuana, Mexico for these treatments. The FTC complaint asserts that the treatments consists of exposing consumers to the "Zoetron machine," a device which purportedly uses a pulsed magnetic field to heat and kill cancer cells. The FTC alleges that the device cannot kill cancer cells, and that the claims made for this therapy are false.

A federal district court in Chicago has issued an injunction prohibiting these claims, freezing the defendants' assets, and ordering the website to be shut down. Canadian Competition Bureau officials executed a criminal search warrant at premises in British Columbia. Mexican officials closed the clinic.

- Press Release (Complaint): http://www.ftc.gov/opa/2003/02/csct.htm

2002

- Arrests and Search Warrants

  - *Arrest (Montreal) [Toronto Strategic Partnership]*

    On January 17, 2002, the Toronto Police Service arrested a man in Montreal when he attempted to withdraw money associated with an advance-fee sweepstakes fraud. Postal Inspectors identified and interviewed several victims who wired or mailed advance fees, purportedly to prepay U.S. Customs fees and taxes in order to collect multi-million dollar prizes. Victims believed U.S. Customs and IRS officials had directed them to send the money. The telephone numbers used by the telemarketers in this scheme were associated with over 400 complaints received by PhoneBusters in Canada. Two of the victims, ages 74 and 81, lost a combined total of $165,000. This case was a result of a joint investigation conducted by the U.S. Postal Inspection Service and Canadian law enforcement authorities with the Toronto Strategic Partnership.

- *Arrests/Search Warrants (Hamilton) [Toronto Strategic Partnership]*

  On June 14, 2002, the Royal Canadian Mounted Police (RCMP) Hamilton, Ontario Detachment executed search warrants and arrested three Canadian nationals who operated an advance-fee loan fraud that targeted U.S. citizens. Investigation has revealed the three suspects led a telemarketing organization which operated out of the Hamilton, Ontario metropolitan area and employed at least ten additional telemarketers. The telemarketers advertised in U.S. publications and on the Internet low interest loans regardless of credit history. They also established multiple mail drop addresses in the United States and Canada. Victims were falsely led to believe by telemarketers posing as loan brokers that they were based in the United States. Domestic area code telephone numbers were simply voice mail accounts or forwarded to Canada. More than 400 U.S. victims have been identified to date, and lost on average $500 each to this promotion.

- *Arrests/Search Warrants (Toronto) [Toronto Strategic Partnership]*

  On June 6, 2002, the Toronto Strategic Partnership Task Force, composed of agents from the Toronto Police Service, Ontario Provincial Police, and U.S. Postal Inspection Service, executed search warrants at four Toronto residences and arrested 11 Canadians associated with an advance- fee loan fraud telemarketing promotion. During these actions, agents also found 4 guns – including 3 semi-automatic handguns and a Mac10 sub-machine gun -- a machete, a bulletproof "police" vest and ID, a quantity of marijuana and $66,000 cash. The raids were the culmination of an 18-month investigation dubbed "Project Mile High," into more than 20 fraudulent loan and associated insurance companies operating in Toronto. Investigation revealed the suspects defrauded thousands of U.S. citizens of more than $5 million over a period of 18 months. Loans were advertised regardless of credit history in U.S. publications. Victims who responded were told by telemarketers that they would have to front an advance fee in order to prepay purported insurance to guarantee the loans. Victims were directed to mail U.S. Postal Service money orders to U.S. and Canadian mail drops, or wire money via Western Union. No loans were ever issued.

- *Arrests/Search Warrants (Toronto/Maryland)*

  On October 21 and 22, 2002, search and seizure warrants were executed at the offices of an advance-fee credit card offer boiler room by the Toronto Police Service and Postal Inspectors. Arrest warrants were also served on four suspects. All four were charged with false or misleading representations; conspiracy to commit indictable capital offense; fraud over $5,000; and possession of property over $5,000. The four were arrested for their parts in operating a major cross border fraud telemarketing scheme involving more than 100,000 U.S. citizens who paid an advance fee for these credit cards. U.S. consumers were targeted and contacted via telephone and promised unsecured Visa/MasterCard credit cards with various credit limits ranging from $1,000 to $3,000 for a $199 to $299 advance fee. Consumers were asked to provide checking and/or savings account information to allow for the debiting of their accounts for this fee. Accounts of consumers were then debited by a contracted Automated Clearing House (ACH) processor. Consumers never received the promised credit card, but instead received a fulfillment packet of benefits that contained credit applications, information on banks that provide credit cards, computer offers, cell phone offers, satellite dish offers, and other types of coupon offers. The fulfillment packages were routinely sent via U.S. Mail from a Baltimore, MD mailing house. Losses are estimated to be approximately $5.5 million. This case received extensive news coverage by the Canadian press and television news services.

  On November 14, 2002, a federal search warrant was executed at the offices of the Maryland company that provided the fulfillment packages for the aforementioned advance credit card fee scheme. The fulfillment packages were sent to consumers via U.S. Mail. Records and documents obtained during the search warrant provided information related to this company's financial situation. From November 18 through 25, 2002, federal seizure warrants were obtained for related bank accounts. These seizures netted $1,032,477.40 in proceeds from suspected illegal telemarketing operations

- *Search Warrants (South Carolina) [Toronto Strategic Partnership]*

On April 22, 2002, federal search warrants were executed on the residence and business addresses of a South Carolina man. The investigation related to a scheme to distribute deceptive sweepstakes promotions that target the elderly. Boiler rooms used for this scheme were operated out of Montreal, Canada. The deceptive sweepstakes promotion represents that the recipient is entitled to cash, merchandise or a vehicle by completing and returning, by mail, a claim form with their telephone number. Claim forms were mailed to various post office boxes located in North Carolina. Most respondents mailed a fee ranging from $9.95 to $14.95, which entitled them to a discount coupon booklet. Individuals responding to the initial promotion were later contacted by a telemarketer and informed that they had won a contest. Victims were told to wire transfer advance fees to Montreal to cover purported taxes or customs duties on their winnings. This telemarketing operation generated approximately $200 million in funds from over 40,000 U.S. victims. The case was jointly investigated by the U.S. Postal Inspection Service, U.S. Customs, North Carolina Attorney General's Office, and the Royal Canadian Mounted Police.

- *Search Warrant (Toronto)*

On December 3, 2002, a search and seizure warrant was executed at the offices of a Canadian citizen in Toronto, Ontario, Canada. The search was conducted by the Royal Canadian Mounted Police, Commercial Crimes Unit, Toronto West Detachment, and was based on a Mutual Legal Assistance Treaty (MLAT) request prepared by the Postal Inspection Service and submitted to the U.S. Attorney's Office in the Middle District of Pennsylvania. The search and seizure warrant authorized RCMP officers, with assistance from Postal Inspectors, to seize voluminous records relating to several suspect companies. The investigation has revealed that the Canadian suspect operated numerous telemarketing operations from Toronto, Canada, and which targeted U.S. consumers. Victims were promised unsecured Visa/MasterCard credit cards with credit limits ranging up to $2,500. The victims were charged an advance fee ranging from $179 to $199 in order to receive the promised credit card. Victim bank accounts were debited by various Automated Clearing House (ACH) processors that were contracted by the Canadian suspect. Victims received a fulfillment packet which contained an application form, a booklet entitled "Today's Credit Solutions", and various coupon books.

No consumer is known to have received a credit card through any of these promotions. The loss is estimated to exceed $3 million. Incident to the execution of the search and seizure warrants, the Federal Trade Commission (FTC), Chicago, IL office began to enforce a Temporary Restraining Order (TRO) filed against the Canadian suspect and his companies. The TRO prevents this individual from contacting consumers in the United States to promote anything with an advance fee, and prevents the ACH companies from releasing any of the funds. The FTC order also freezes assets located in the suspect's U.S. bank accounts.

- Criminal Prosecutions - Identity Theft

  - *Regina v. Taft* (B.C. Super. Ct., pleaded guilty June 7, 2002)

    This criminal case, brought by the British Columbia Attorney General, stemmed from the identity theft-related activities of an American citizen who remained illegally in Canada (Anthony B. Taft). Between November 1998 and August 2000, Taft obtained personal information from individuals by running advertisements in the "Help Wanted" sections of local newspapers and inducing respondents to provide copies of identification papers. Taft then forged or applied for identification in the names of the victims, opened bank accounts under their names, and deposited counterfeit checks in the accounts and withdrew funds. Over a two and one-half month period, Taft obtained almost $80,000 CA in cash by cashing counterfeit checks and making withdrawals. In Québec, Taft, using the name of one of his victims, also ran a website for making false identification documents. Police later found among Taft's personal materials both American and Canadian passports of real people; Taft was able to insert his photograph onto the passports so that he could travel at will under other victims' names.

    On June 7, 2002, after spending 12 months in pretrial custody, Taft pleaded guilty to 23 fraud-related offenses. On June 26, 2002, Taft was sentenced to a total of three months, after the sentencing judge determined that the sentence, coupled with his pretrial detention, was the equivalent of a 27-month sentence. On February 11, 2003, the British Columbia Court of Appeal upheld the sentence.

- Criminal Prosecutions - Telemarketing Fraud

  - *Ontario Case* (Ontario Superior Court 2002)

    On April 19, 2002, three Canadian citizens appeared at a Province of Ontario Regional Court and were charged with conspiracy and fraud over $5,000. The charges relate to a cross-border telemarketing operation that solicited advance fees from victims who allegedly won a sweepstakes. The charges are a result of a joint investigation conducted by the Philadelphia Division of the U.S. Postal Inspection Service and the greater Toronto area Royal Canadian Mounted Police. The telemarketers posed as Georgia lottery officials, and falsely told prospective victims that they had won a Cadillac and cash prize. Victims were required to mail an advance fee to cover purported tax, license and transportation expenses. Mail drop addresses in Ontario were used to receive victim payments. These payments were then forwarded to Quebec where they were cashed. Approximately 100 victims lost over $250,000 to this scheme from September to December 2001.

  - *Regina v. Plunkett* (Ontario Superior Court, 2001) [Toronto Strategic Partnership]

    On October 18, 2000, the Partnership, with assistance from TICO, executed a search warrant on Carnival Tours and Signature Weekends, a telemarketing company operating under the umbrella of the SW Group. Thirty individuals were arrested and one person was charged with fraud. Consumers were contacted to participate in a "travel survey" and asked about their use of credit cards to pay for vacations. They were allegedly entered in a draw for a free cruise, for taking part in the survey. The "winners" were required to pay $199 U.S. by credit card, to secure the trip. The accused is also before the court on charges under the Travel Act involving Signature Weekends. Consumer losses are estimated at CA $2.5 million. Approximately $250,000 was seized for return to victims.

    On September 20, 2001, Jason Plunkett pleaded guilty and was sentenced to 2 years less a day, and required to make restitution of $105,558.72 to banks and to forfeit $96,113.28 to the Toronto Police Service.

- *United States v. Anekwu*, No. 01-0912M (C.D. Cal., criminal complaint filed April 24, 2002) [Emptor]

  This criminal case, brought by the United States Attorney's Office in Los Angeles, charges one defendant (Henry Anekwu) with fraud-related offenses pertaining to an alleged foreign lottery scheme that operated under the name Platinum International. The defendant's scheme allegedly involved passing counterfeit business checks to U.S. citizens. As of April 2003, the United States expects to submit an extradition request to Canada.

- *United States v. Arcand and Galway*, No. CR 02-940(A)-DT (C.D. Cal., indictment filed August 29, 2002) [Emptor]

  This criminal case, brought by the United States Attorney's Office in Los Angeles, charges two defendants (Philip Arcand and Roberta Galway) with fraud-related offenses pertaining to an alleged credit-card protection scheme that operated under the names American Card Services and Farpoint Services International. Victims of the scheme, who lived as far away as Hawaii, Michigan, West Virginia and California, suffered estimated losses of approximately US $3 million. After their indictment in August 2002, the defendants were arrested in Las Vegas, where they had moved. On March 10, 2003, Galway pleaded guilty to mailing lottery tickets or related matter. On April 2, 2003, a jury found Arcand guilty of mail fraud and mailing lottery tickets or related matter. Arcand is now awaiting sentencing.

  In a related civil action in October 2001 [see FTC v. Farpoint Services International below], the FTC brought suit against Arcand, Galway, and Phillip Arcand. In September 2002, a stipulated permanent injunction was signed with the FTC. Under the terms of the injunction, the defendants were barred from selling credit-card protection and agreed not to misrepresent any product and to pay civil redress of $436,000.

  - Press Release (Civil Action): http://www.ftc.gov/opa/2001/10/ditch.htm

- *United States v. Asiegbu, et al*., No CR 02-673 (C.D. Cal., indictment filed June 27, 2002)

  This criminal case, brought by the United States Attorney's Office in Los Angeles, charges five defendants (Natty Asiegbu, Robert Smith, Geoffrey Crozier, Joshua Danielson, and Charles Dike) with various fraud-related offenses pertaining to an alleged lottery scheme that included some aspects of a recovery scam. An extradition request is pending in Canada.

- *United States v. Farhatullah, et al*., No. CR 02-1175-PA (C.D. Cal., indictment filed October 2002) [Emptor]

  This criminal case, brought by the United States Attorney's Office in Los Angeles, charges three defendants (Mohammad Farhatullah, William Robertson, and Judy McCluskey) with fraud-related offenses pertaining to an alleged foreign lottery scheme that operated under the name Tullah Holdings Inc. Farhatullah and McCluskey were arrested in Blaine, Washington. McCluskey subsequently signed a plea agreement, and Farhatullah is scheduled to be tried on April 22, 2003. A request for Robertson's extradition from Canada is in preparation.

- *United States v. Franco*, No. 02-2655M (C.D. Cal., criminal complaint filed December 17, 2002) [Emptor]

  This criminal case, brought by the United States Attorney's Office in Los Angeles, charges one defendant (Alexander Franco) with fraud-related offenses pertaining to an alleged lottery scheme. A request for extradition from Canada will be filed.

- *United States v. Karim (aka Dillon Sherif)*, No. CR 01-2101M (C.D. Cal., indictment filed October 2001) [Emptor]

  This criminal case, brought by the United States Attorney's Office in Los Angeles, charges one defendant (Nuraldin Shareef Karim, aka Dillon Sherif) with fraud-related charges pertaining to an alleged foreign lottery scheme, targeting U.S. victims, that operated under the name Global Dreams Services Ltd. In October 2001, at the time of Karim's indictment, a boiler room in Vancouver was searched pursuant to the British Columbia

Trade Practice Act. In connection with these proceedings, a total of $1.1 million was restrained at financial institutions; residential property in Vancouver and Whistler, British Columbia, valued at $1.4 million was restrained; and several luxury vehicles valued at approximately $380,000 were seized. In addition, Karim was arrested in Canada and extradition proceedings initiated.

After Karim was released on bail with CA $200,000 surety in British Columbia, he fled the jurisdiction. Karim is now considered a fugitive by law enforcement authorities, who have issued a worldwide alert through Interpol.

- *United States v. Levine* (D. Mass., arrested February 2001) [COLT].

  This criminal case, brought by the U.S. Attorney's Office in Boston, stems from the February 2001 arrest of a U.S. citizen (Mark Levine) by members of Project COLT, in connection with an investigation of a Montreal-based telemarketing operation. Levine, who was wanted in North Carolina in connection with another telemarketing fraud-related case, ultimately was sentenced to 57 months imprisonment in North Carolina. On September 16, 2002, Levine was sentenced to 75 months imprisonment in Boston – to run consecutively to the 57-month sentence previously imposed – and restitution of $1.3 million. As a result, Levine will be required, under federal sentencing guidelines, to serve 11 years imprisonment (less "good time" credit).

- *United States v. Smida, et al*., No. CR 02-541 (C.D. Cal., indictment filed May 29, 2002) [Emptor]

  This criminal case, brought by the United States Attorney's Office in Los Angeles, charged five defendants (Imre Smida, David Deland, Guy Deland, Brian Brunton-Guerrard, and Robert Seaton) with fraud-related offenses pertaining to an alleged lottery scheme. A request for the defendants' extradition from Canada is in preparation.

- *United States v. Taillon et al.* (D.N.H., indictment filed October 7, 2002)

This criminal case, brought by the United States Attorney's Office in Concord, New Hampshire, charged a total of 14 defendants (including Joseph Taillon, David Johnson, and Norman Redler) with conspiracy to commit racketeering and mail fraud conspiracy, and a total of 15 defendants with conspiracy to commit wire fraud, in connection with a telemarketing fraud scheme targeting the elderly. On April 30, 2002, the Canadian partners in Project COLT had arrested 17 persons in the Montreal, Longueuil, Laval**,** and Prévost areas. These persons were suspected of belonging to a telemarketing fraud network. This series of arrests required the participation of 125 police officers. The investigation by the COLT partners established that the accused defrauded their American victims by leading them to believe that they had won substantial lottery prizes. Approximately 100 U.S. residents have allegedly been defrauded of more than US $6 million.

In a parallel civil forfeiture action filed on October 18, 2002, the United States Attorney's Office, using provisions in the USA Patriot Act, seized $4.5 million from the accounts of several Middle Eastern banks. In January 2003, the defendants, all Canadian citizens, were subject to provisional arrest in Canada.

- Press Release (Provisional Arrest): http://www.grcquebecrcmp.com/pages/english/con_p_m_e/pag_m_6p1_e.html

- *United States v. Mornan*, No. 1-CR-02-242-01 (M.D. Pa., superseding indictment filed Feb. 5, 2003)

On October 2, 2002, a Middle District of Pennsylvania Grand Jury returned an 18-count indictment naming a Canadian national, Christopher Mornan, as the co-owner and manager of 12 advance-fee loan broker/insurance company telemarketing promotions, which operated during the period of December 1997 through December 2001. Low interest loans were offered regardless of credit history. Purported loan brokers instructed loan applicants to mail postal money orders to fictitious insurance companies in Canada. The victim remittances were sent to mail drop addresses in Canada, and routinely forwarded to other mail drops to further conceal the identity of the telemarketers. New mail drops, cell

phones and Ontario business registrations were procured for each operation using fictitious names. The indictment charged that more than 500 victims lost in excess of $1 million.

A superseding indictment was filed against Mornan on February 5, 2003. On April 14, 2003, Mornan was found guilty at trial on 15 counts of criminal conspiracy, wire fraud, and mail fraud.

- Civil and Administrative Enforcement Actions - Telemarketing Fraud

  - *FTC v. 564196 B.C. Ltd. doing business as International Brokers Limited*, No. 02-CV-1228 (W.D. Wash., civil complaint filed June 10, 2002) [Emptor]

    The FTC filed this action against three individual defendants and one corporation based in British Columbia in connection with deceptive telemarketing scheme involving foreign lotteries, primarily the Australian lottery. British Columbia officials froze $211,000 in assets.

    - Press Release (Complaint): http://www.ftc.gov/opa/2002/06/crossborder.htm

  - *FTC v. 1st Beneficial Credit Servs. LLC, et al.*, No.: 1:02 CV 1591 (N.D. Ohio, civil complaint filed Aug. 14, 2002) [Toronto Strategic Partnership]

    As part of the FTC's "Operation No-Credit" sweep, the FTC charged several corporations and individuals operating out of the Toronto, Canada area with violating the FTC Act and the Telemarketing Sales Rule in connection with deceptive telemarketing scheme. The defendants' telemarketers called U.S. consumers and offered guaranteed Visa or MasterCard credit cards with substantial credit limits for a $199 advance fee. The FTC's complaint alleges that consumers never received the promised credit card.

    - Press Release (Complaint): http://www.ftc.gov/opa/2002/09/opnocredit.htm

  - *FTC v. Consumer Alliance Inc. et al.*, No.: 02-C-2429 (N.D. Ill., civil complaint filed Apr. 4, 2002) [Toronto Strategic Partnership]

In this civil action, the FTC charged three individuals and four corporations that operated as a common enterprise in Ontario, Canada with deceptively marketing worthless credit-card protection programs to U.S. consumers in violation of the FTC Act and the Telemarketing Sales Rule. Specifically, the FTC alleged that the defendants in the case telephoned consumers and offered low interest credit cards, but never provided consumers with a credit card. According to the FTC, during the sales pitch, the defendants' telemarketers allegedly misled consumers by saying that: the telemarketers were affiliated with, or calling from, Visa or MasterCard, or on behalf of the consumers' credit card issuers; consumers could be held fully liable for any unauthorized charges made on their credit cards if they did not purchase this protection; and consumers would only have to pay a small fee for the service - typically $2.99 or $3.49 - instead of the $299 to $349 the defendants actually charged. In addition, the complaint alleged that in other calls the defendants' telemarketers promised U.S. consumers a credit card with a low interest rate, or a low interest rate on the consumers' existing credit card, in exchange for a $349 or $399 fee. In fact, according to the FTC, those consumers only received a list of banks to which they could apply for credit cards. The FTC also alleged that the defendants also placed unauthorized charges on the credit cards of many U.S. consumers. The Ontario Provincial Police, Anti-Rackets Section, which has filed criminal charges against some of the defendants, and other members of the Toronto Strategic Partnership, provided assistance to the FTC in its investigation.

- Press Release (Complaint): http://www.ftc.gov/opa/2002/04/consumeralliance.htm

- *FTC v. D&C National Holdings, Ltd. et al.*, No.: CV02-1134 (W.D. Wash., civil complaint filed May 23, 2002) [Emptor]

In this civil action, the FTC charged three individuals and two corporations based in British Columbia with violating the FTC Act and the Telemarketing Sales Rule, in connection with a scheme to sell both bogus British bonds and foreign lottery tickets to consumers in the United States and the United Kingdom. The FTC's action was coordinated with the British Columbia Director of Trade Practices, who filed an action against

the defendants and several additional related individuals and companies in British Columbia in May 2002. The Director of Trade Practices obtained an order authorizing a raid on defendants' business premises and an order freezing defendants' Canadian bank accounts and personal property including 41 luxury vehicles. $2.8 million in cash, property, and luxury vehicles was restrained. Subsequently, in December 2002, a commercial mail center (Midtown Mailboxes) that was directly linked to D. & C. was searched under the Trade Practice Act, with a further restraint of $660,000 and a cash seizure of $65,000. The investigation is ongoing.

- Press Release (Complaint): http://www.ftc.gov/opa/2002/06/crossborder.htm

- *FTC v. Efficient Telesales Services Inc., dba U.S. Credit Servs. and U.S. Direct Benefits and Savings et al.*, No. 02C 377 (E.D. Ill., civil complaint filed May 28, 2002) [Toronto Strategic Partnership]

  In this civil action, the FTC charges that the defendants, an Ontario-based corporation and its principal, Leonora Khan, telemarketed low interest credit cards to U.S. consumers in violation of the FTC Act and the Telemarketing Sales Rule. Defendants claimed to offer pre-approved VISA or MasterCard credit cards with interest rates around 3.9%, no annual fees, and credit limits of $2,500 or $5,000. Consumers did not receive the promised credit cards. The U.S. district court in Chicago issued an injunction prohibiting the deceptive practices and freezing assets. In conjunction with the FTC filing, the Ontario Provincial Police, the Toronto Police Service and the York Regional Police Service arrested defendant Leonora Khan and executed a search warrant on U.S. Credit's business premises.

  - Press Release (Complaint): http://www.ftc.gov/opa/2002/06/crossborder.htm

- *FTC v. First Capital Consumers Group et al.*, No.: 02C 7456 (N.D., civil complaint filed Oct. 17, 2002) [Toronto Strategic Partnership]

  In this civil action, the FTC charged a Toronto-based company, operating eight telemarketing boiler rooms, and several individual defendants with

operating a fraudulent advance-fee credit card business in violation of the FTC Act and the Telemarketing Sales Rule. The defendants' telemarketers told consumers that they would receive pre-approved MasterCard or Visa credit cards with low interest rates, credit limits of $2,000 or $2,500, and no annual fees. Consumers paid the defendants by agreeing to have their bank accounts debited for the advance fee of $189 to $219. The FTC alleged that none of the consumers who paid the defendants received the promised credit cards. A federal district court in Chicago entered an injunction prohibiting false claims and freezing the defendants' assets. The FTC investigated this case in conjunction with the Canadian Competition Bureau, which has filed criminal charges against some of the defendants. The Toronto Strategic Partnership provided additional assistance during the investigation.

- Press Release (Complaint): http://www.ftc.gov/opa/2002/10/firstcap.htm

- *FTC v. Full House/Royal Flush System Network, Inc. et al.*, No.: 2:02 CV 1085 (W.D. Wash., civil complaint filed May 15, 2002) [Emptor]

  In a civil action related to *United States v. Okike and Steeves* (see below), the FTC filed a civil complaint against defendants based in British Columbia, in connection with a deceptive telemarketing scheme involving foreign lotteries. The defendants' telemarketers persuaded consumers that they would win the German, Spanish, or other foreign lotteries if they paid the defendants to play on their behalf. Consumers were also told they had won large sums of money but needed to pay a fee to collect their winnings. Defendants also ran a recovery room scheme advising consumers that for a fee, the defendants would recover money the consumers had lost in other scams. Two of the individual defendants, Wilson Okike and Basil Steeves (see below), were arrested in the United States, have pleaded guilty to criminal wire fraud charges, and are serving time in U.S. prisons. The British Columbia Director of Trade Practices has frozen or filed claims against approximately $926,000 in assets in Canada, while the U.S. Department of Justice holds another $218,000 in forfeited assets in the United States.

- Press Release: (Complaint): http://www.ftc.gov/opa/2002/06/crossborder.htm

- *FTC v. Hanson Publications, Inc. et al.*, No. 1:02 CV 2205 (N.D. Ohio, civil complaint filed Nov. 8, 2002)

  In this civil action, the FTC charged three Canadian telemarketing companies, which operated boiler rooms in Quebec and Ontario that employed more than 400 people, with engaging in fraudulent business practices in the sale of business directories and non-durable office supplies in violation of the FTC Act and the Telemarketing Sales Rule. The FTC obtained a temporary restraining order and a preliminary injunction freezing the defendants' assets to preserve them for consumer redress, and requiring the defendants to account for their assets, including assets located abroad. Certain of the defendants to the action then filed a lawsuit against the Crown in the Superior Court of Justice in Ontario requesting, inter alia, that they be permitted to use funds in Canada to pay Canadian counsel for representation in related criminal proceedings commenced by Canada's Competition Bureau. The Canadian court denied the defendants' application in February 2003.

  - Press Release (Complaint): http://www.ftc.gov/opa/2002/11/handson.htm

- *FTC v. Pacific First Benefit L.L.C. et al.*, No. 02C8678 (N.D. Ill., civil complaint filed Dec. 2, 2002) [Toronto Strategic Partnership]

  This FTC action charges a Toronto-based company, operating under several names, with promising consumers a major credit card, and charging an advance fee for it, but never delivering the credit card in violation of the Federal Trade Commission Act and the Telemarketing Sales Rule. According to the FTC, the defendants targeted U.S. citizens who had no credit or bad credit with their advance-fee credit card offer. According to the FTC, the defendants never provided consumers with the promised credit cards and are not authorized by VISA or MasterCard to issue credit cards to the public. The FTC alleges that this business enterprise sold only to U.S. consumers, and estimates that total sales exceeded $5 million. A U.S. federal court has issued an injunction

prohibiting the defendants from making deceptive claims and freezing the assets of the defendants to preserve funds for possible consumer redress.

- Press Release (Complaint): http://www.ftc.gov/opa/2002/12/firstfederal.htm

- *FTC v. Dillon Sherif et al.*, No. 2:02 CV 00294 (W.D. Wash., civil complaint filed Feb. 7, 2002) [Emptor]

  In a civil action related to *United States v. Karim* (see above), the FTC filed against several British Columbia-based individuals, including Nuraldin Shareef Karim, aka Dillon Sherif, and corporations that targeted elderly consumers, on telemarketing fraud-related charges. The action alleged that the defendants sometimes tried to sell consumers shares in foreign lottery tickets, other times claiming that consumers had won millions in an Australian or Spanish lottery or a "give-away" sponsored by the Spanish royal family. According to the FTC's complaint, the defendants told consumers that in order to receive their winnings, they had to first send money - described variously as taxes, duties, or currency conversion costs - to the defendants. The initial payments ranged from $250 to $999 and consumers who paid were frequently contacted again for more money. The FTC coordinated its investigation with the British Columbia Ministry of Public Safety and Solicitor General, who filed a civil action against the defendants in Canada and froze over $1 million of their assets and seized property and vehicles in their names. Trial in the FTC's action is currently set for August 2003. As described above in *United States v. Karim*, Karim/Sherif is currently a fugitive.

  - Press Release (Complaint): http://www.ftc.gov/opa/2002/02/dillon.htm

- *FTC v. World Media Brokers Inc. et al.*, No.: 02C-6985 (N.D. Ill., civil complaint filed Sept. 30, 2002) [Toronto Strategic Partnership]

  In this civil action, the FTC charged a group of related companies operated by six Canadians that operated an illegal foreign lottery scheme with violations of the FTC Act and the Telemarketing Sales Rule. In its civil complaint, the FTC alleged that the telemarketers told its mostly

elderly victims - falsely - that it is legal for U.S. consumers to buy Canadian lottery tickets, and that by investing with them, the consumers had a very good chance of winning the Canadian lottery and that telemarketers told many consumers that it is legal for U.S. consumers to buy Canadian lottery tickets. They told some consumers that they had already won a large prize and that consumers should send them money to redeem their winnings. The FTC alleged that total sales to consumers were at least $25 million. At the request of the FTC, a U.S. district court has temporarily barred the defendants from selling tickets, chances, or any foreign lottery chances to residents of the United States; barred deceptive claims about the chances of winning the Canadian lottery; prohibited misrepresentations or omissions about material facts; and ordered an asset freeze to preserve funds for consumer redress. The United States Department of Justice, Office of Foreign Litigation, has brought a parallel civil action in court in Canada, enjoining the deceptive practices and freezing the assets of defendants.

- Press Release (Complaint): http://www.ftc.gov/opa/2002/12/ems.htm

- *State v. AXS Marketing and Pinto* (Crawford Co. Circuit Ct., Mo., civil action filed October 2, 2002)

  This civil action, brought by the Missouri Attorney General, charged AXS Marketing, a Montreal telemarketing company, and its owner, Oren Pinto, with violating Missouri consumer protection laws by making numerous misrepresentations in telemarketing calls. The defendants allegedly asking for credit card, bank account, and Social Security number information under false pretenses, including telling consumers that the telemarketers are working with the Attorney General's Office to try to stop fraud.

  - Press Release (Civil Action): http://www.ago.state.mo.us/newsrls/2002/100302.htm

- *State v. Xentel Inc.* (Pa., settlement announced December 2002)

  This civil action, brought by the Pennsylvania Attorney General, charged Xentel, Inc. of Alberta with using false and misleading tactics during telephone fund-raising efforts for firefighters in 1999 and 2002. In December 2002, the Pennsylvania Attorney General announced a settlement with Xentel. Under the terms of the settlement, Xentel must pay $14,000 in restitution, $3,000 in civil penalties, and $3,000 for the Commonwealth's investigatory costs. In addition, the agreement requires the company to (1) permanently cease operating in violation of Pennsylvania's Charitable Purposes Act and the Unfair Trade Practices and Consumer Protection Law; (2) issue refunds to consumers who were victimized and delete their names from the company's call list; (3) provide the Commonwealth with records or documents regarding future consumer complaints; and (4) furnish taped copies of solicitations during phone room inspections by the Attorney General's Office.

- Civil and Administrative Enforcement Actions - Health Fraud

  - FTC v. 9068-8425 Quebec, Inc. d/b/a Bio Lab, Cellu-Fight, and Quick Slim, and Jean-Francois Brochu, Civil Action No. 1:02-CV-1128 (N.D.N.Y., civil complaint filed Sept. 3, 2002)

    In this civil action, the FTC charged a Canadian corporation operating in the United States under the name "Bio Lab" and its president, Jean-Francois Brochu, with deceiving consumers through false advertising for their weight-loss and cellulite-treatment products in violation of the FTC Act. In its civil Complaint filed in the Northern District of New York, the FTC alleged that defendants, using mainstream U.S. print media and the Internet, targeted U.S. consumers by advertising and selling "Quick Slim," a purported weight-loss product claimed to cause rapid and substantial weight loss without dieting or exercise, and "Cellu-Fight," a cellulite-treatment product claimed to completely eliminate cellulite without any effort by users. Bio Lab also advertised and sold Cellu-Fight through direct mail brochures sent to Quick Slim purchasers. On September 6, 2002, the district court issued a temporary restraining order prohibiting the advertising of defendants' products and freezing their asset, and on October 11, 2002 the parties entered into a Stipulated Preliminary

Injunction that continued the ban on the dissemination of defendants' deceptive advertising claims, extended the asset freeze, and provided the FTC with expedited discovery. Since the FTC filed its action, Bio Lab has ceased doing business. The Canadian Competition Bureau provided the FTC with assistance in this case.

- Press Release (Complaint): http://www.ftc.gov/opa/2002/09/biolab.htm

2001

- Arrests and Search Warrants - Africa-Related/Telemarketing Fraud

  - *Telemarketing Fraud Case*

    On July 10, 2001, the RCMP arrested three individuals who were charged with conspiracy to commit fraud, fraud against the general public, and laundering the proceeds of crime. The three defendants allegedly participated in a "4-1-9" advance-fee scheme that involved both initial solicitations from Nigeria and followup contacts from a boiler room in Toronto. These arrests were the culmination of a three-year investigation that involved the RCMP and the FBI's Operation Canadian Eagle, in association with the US Secret Service. As of the time of the arrests, the RCMP had identified more than 300 victims from around the world. Most victims were from the United States, although some victims were identified in Europe and Asia. Individual losses range from $52,000 US to more than $5 million US.

    - Press Release (Arrests): http://www.rcmp-grc.gc.ca/news/2001/nr-01-11.htm

- Arrests and Search Warrants - Securities Fraud

  - *"Stock Swap" Schemes*

    On February 27, 2001, after a 20-month investigation by the RCMP, the FBI, and the Ontario Securities Commission, six persons were arrested and charged with conspiracy to commit fraud, among other charges, in

connection with an elaborate "stock swap" scheme operating in the Toronto area. At the time of these arrests, two other persons had warrants outstanding against them. The RCMP estimated that losses from approximately 150 victim investors from around the world total approximately $4 million, with individual losses ranging from $1,500 to $675,000.

- Arrests and Search Warrants - Telemarketing Fraud

  - *Sweepstakes Fraud [Toronto Strategic Partnership]*

    On July 16, 2001, three people were arrested and charged with fraud over $5,000, relative to a sweepstakes scam perpetrated on a 90-year-old victim in Toronto. Partnership investigators received information that the accused were driving from Montreal to collect a cash deposit from the victim who had been told that she had won $800,000 in the Prestige Inc. Sweepstakes. The telemarketers escorted the victim to the bank to obtain $5,000. Only $500 was withdrawn and that money was returned to the victim when the arrests were made. Investigation revealed that the victim had lost over $8,000 to these Montreal based telemarketers during the previous year.

- Criminal Prosecutions - Telemarketing Fraud

  - *United States v. Dorsey and German*, No. SA CR 01-161-AHS (C.D. Cal., indictment filed September 26, 2001)

    This criminal case, brought by the United States Attorney's Office in Los Angeles, charged two defendants (Terry Dorsey and Shelly German) with fraud-related offenses pertaining to a "rip and tear" lottery scheme operating out of Montreal. Both defendants were extradited from Canada and pleaded guilty. Dorsey received a sentence of 63 months imprisonment and Germann received a sentence of 36 months imprisonment.

  - *United States v. Impellezzere* (D. Ariz., arrested June 7, 2001)

This criminal case, brought by the United States Attorney's Office in Phoenix, stems from the arrest and charging of Angelo Impellezzere, a resident of Quebec, while he was visiting an assisted living facility to meet with an 84-year-old telemarketing fraud victim. Impellezzere posed as an undercover Canadian police officer, using an alias, and told the victim, who had already lost $80,000 to criminal telemarketers, that he needed another $10,000 from her so that her funds could be traced back to the people who had defrauded her of the $80,000. He was arrested when he arrived after midnight at the victim''s assisted-living facility, allegedly to pick up not only her $10,000 but another $7,500 that he had persuaded another victim to wire to her so that he could pick up the funds at the same time. On November 26, 2001, Impellezzere pleaded guilty to one count of money laundering in connection with the alleged scheme. On February 20, 2002, he was sentenced to 21 months imprisonment.

- Press Release (Sentence): http://www.usdoj.gov/usao/az/azpress/2002-041.pdf
- Congressional Testimony (2001): http://govt-aff.senate.gov/061501_warlow.htm

- *United States v. Morin et al.* (D. Mass., arrested February 9, 2001; indictment filed March 8, 2001; superseding indictment filed June 2001) [COLT]

  This criminal case, brought by the United States Attorney's Office in Boston, stems from the arrest of Denis Morin (aka Denis Baribeau), the manager of a large prize- and recovery-room telemarketing operation in the Montreal area, at Walt Disney World in Florida. In a coordinated series of actions, Canadian law enforcement authorities arrested 26 other people connected with the operation. Morin and two other individuals located in Laval, Quebec, had run the scheme, in which callers falsely represented themselves as government officials, such as IRS and U.S. Customs employees and judges, as well as lawyers. The victims were located across the United States. During a three-week period in January 2001, more than 1,000 phony telemarketing calls were placed from the location in Quebec, resulting in 46 Americans forwarding funds totaling more than $436,000 to Canada, and 208 other American prospects indicating that they were intending to send funds totaling another $2.9

million. No victim who forwarded money in response to the calls ever recovered any money or received any funds or prizes.

Morin, who operated this scheme out of various locations for almost four years, was subsequently indicted in the District of Massachusetts on charges of conspiracy, mail fraud, and wire fraud. The indictment alleges that the operation targeted principally senior citizens and other vulnerable members of society. One of the alleged boiler room managers arrested in Montreal, Vasilios Kolitsidas, was (as of June 2001) also a fugitive from a federal indictment in the Middle District of Florida. Baribeau subsequently pleaded guilty to conspiracy and wire fraud. On March 26, 2003, Baribeau was sentenced to 10 years imprisonment and restitution of $1,277,525.49. In imposing sentence, the judge noted the "despicable crime" involved, particularly because of its impact on older and defenseless people.

- Congressional Testimony (2001): http://govt-aff.senate.gov/061501_warlow.htm
- PhoneBusters News Release (Sentencing): http://www.PhoneBusters.com/Eng/Charges_Arrests/March_27_2003.html

- *United States v. Katz*, Nos. CR 010373 and 010374 (D. Md., indictments filed July 10, 2001)

This criminal case, brought by the United States Attorney's Office in Baltimore, Maryland, stems from two indictments against seven individuals and a company on various fraud-related charges relating to telemarketing fraud schemes that defrauded more than 27,000 consumers of more than $3.3 million. According to the Indictments, the lead defendant, Joel Katz, operated a telemarketing business and controlled bank accounts in the names of the following corporations: Telennium, Ltd.; Southern Belle Security Systems, Inc.; Bulk Long Distance, Inc.; Kiss'n Tel Communications, Inc.; The Money Club, Inc.; Multicard Services, Inc.; and VIP Billing and Collection, Inc. The Indictments also alleged that telemarketing representatives, using scripts written by Katz, spoke on the telephone with consumers to persuade them to purchase programs entitled The Money Club, The Tele-Money Club, etc., for prices

ranging from $49.95 to $149.95. Consumers were told that in exchange for the fee, they could become a member of the club and receive a package of benefits, including a credit card for which the consumer had been "pre-approved," valuable coupons and discounts. The telemarketing representative would persuade the consumer to agree to the automatic debit of their bank account to pay for club membership. According to the Indictments, the package that was sent to the consumer contained, not a credit card, but some or all of the following items: a list of banks which the consumer had to contact to apply for a card or a bank card application, a coupon package purchased for $3.47 or coupons purchased for $.01 each, a CD Rom for an internet connection purchased for $.37 per CD, and a telephone calling card.

On June 6, 2002, Katz and one of his co-defendants, Judith Lugo, were convicted at trial, after three of their codefendants, who had pleaded guilty to various charges, testified for the government. Katz was convicted on multiple counts of mail and wire fraud, money laundering, and conspiracy; and Lugo on multiple counts of mail and wire fraud and conspiracy. On August 29, 2002, Katz was sentenced to 97 months imprisonment on the money laundering charges, and concurrent 60-month terms of imprisonment on the other counts of conviction; Lugo was sentenced to 51 months imprisonment on her counts of conviction. Two other co-defendants are scheduled to stand trial in May 2003.

- Press Release (Indictment): http://www.usdoj.gov/usao/md/press_releases/press01/katzindcorrection.htm
- Press Release (Conviction): http://www.usdoj.gov/usao/md/press_releases/press02/joel_katz_judith_lugo_convicted.htm
- Press Release (Sentencing): http://www.usdoj.gov/usao/md/press_releases/press02/joel_katz_sentenced.htm

- *United States v. Okike and Steeves*, No. CR 01-16-MM (C.D. Cal., indictment filed January 10, 2001) [Emptor]

  This criminal case, brought by the United States Attorney's Office in Los Angeles, indicted two Canadian citizens and residents of British Columbia (Wilson Okike and Basil Steeves) on 12 counts of wire fraud and six counts of mailing fraudulent materials relating to lotteries. The indictment alleged that Okike and Steeves operated fraudulent telemarketing firms in Vancouver called North Klassen Services, Globallot Services, Royal Flush Ltd., and Intersweeps Management Services, through which they offered foreign lotteries targeting U.S. victims. In December, 2000, Okike and Steeves were arrested in Blaine, Washington while doing banking there. After being indicted in January 2001, both defendants later pleaded guilty to charges of wire fraud and mailing of lottery materials. Okike received a sentence of 84 months imprisonment and Steeves received a sentence of 30 months imprisonment.

  - Press Release (Indictment): http://www.usdoj.gov/usao/cac/pr2001/004.html

- *United States v. Polyak*, No. SA CR 01-51-DOC (C.D. Cal., indictment filed March 14, 2001) [Emptor]

  This criminal case, brought by the United States Attorney's Office in Los Angeles, stems from the arrest of Joseph Polyak on the basis of a criminal complaint, while he was doing banking in Blaine, Washington. Polyak allegedly conducted a foreign lottery scheme, under the names Imperial International Services, Premier International, 591117BC LTD, and ELC Services, that targeted U.S. victims. The scheme allegedly involves calls to elderly victims from British Columbia. Polyak and two other defendants, Brent Fordham and Luke Lillemo, were subsequently indicted on wire fraud charges, as well as the telemarketing fraud sentencing enhancement. After pleading guilty to certain charges, Polyak was sentenced to six months imprisonment. Both Fordham and Lillemo were arrested in Canada on the basis of these charges, and a request for their extradition from Canada is pending.

- Congressional Testimony (2001): http://govt-aff.senate.gov/061501_warlow.htm

- *United States v. Tanguay, et al.*, No. CR 01-139 (C.D. Cal., indictment filed February 15, 2001) [Emptor]

  This criminal case, brought by the United States Attorney's Office in Los Angeles, charged four defendants (Jacques Tanguay, Christina Tanguay, Donna Mata, and Wilfred Veyt) with wire fraud, including the sentencing enhancement for telemarketing fraud, 18 U.S.C. § 2326. Jacques and Christina Tanguay allegedly owned and operated a British Columbia-based lottery operation called, at various times, Global Dividends International, Horizon 2000 Investments International, and Platinum International. Mata and Veyt allegedly managed and were telemarketers in the operation. (In addition, Eduardo Cartagena, the son of Christina Tanguay, was a manager in their operation (see below)). The indictment alleges that during the course of the scheme, which ran from about November 1997 to May 2000, the defendants induced elderly victims to send more than $2.7 million to the operation.

  On January 10, 2003, Jacques and Christina Tanguay were extradited from Canada, after being held in custody since November 28, 2002. Both defendants entered plea agreements in the case that would require them to serve sentences of 10 years imprisonment and 5 years imprisonment, respectively. A request for extradition of the other defendants is pending.

  - Press Release (Extradition): http://www.grcquebecrcmp.com/pages/english/con_p_m_e/pag_m_6g_e.html
  - Congressional Testimony (2001): http://govt-aff.senate.gov/061501_warlow.htm

- Civil and Administrative Enforcement Actions - Telemarketing Fraud

  - *FTC v. 9094-5486 Quebec Inc. dba Consumer Resource Servs*., 01CV 1872 (TJM RFT) (N.D.N.Y., civil complaint filed Dec. 10, 2001, default judgment entered Oct. 21, 2002)

    In this civil action, the FTC charged three individuals and one corporation based in Montreal, Quebec, with violations of the FTC Act and the Telemarketing Sales Rule in connection with a telemarketing operation that supposedly offered free products or services such as a low interest rate credit card or access to unclaimed cash. The defendants told the consumers, many of them elderly, that their credit card numbers were required to receive free goods or services, but that their credit cards would not be charged. The defendants used the information they obtained from the consumers to establish accounts in the consumers' names with online payment services. Defendants then clicked through to online payment services instructed the payment services to charge the consumers' credit cards, generally in the amount of $229, and transfer payment to them. Many consumers who were charged for the CRS package did not receive any products from CRS. Consumers who did receive a CRS package found that it did not contain a credit card or the products promised by the telemarketers. Instead, the package contained a notebook with a few pages of literature, coupons, and a pamphlet of names, addresses, and telephone numbers of companies that may provide free product samples or coupons.

    In October 2002, the FTC obtained a default judgment against the defendants in the amount of $587,388,61. The order also prohibited the defendants from engaging in abusive telemarketing practices.

    - Press Release: (Complaint): http://www.ftc.gov/opa/2001/12/crs.htm

  - *FTC v. Alvin Cordeiro, dba Quick-Checks, 5:01cv20109* (N.D. Ca., civil complaint and stipulated final judgment filed Feb. 6, 2001)

    In this civil action, related to the FTC's 1998 action against Canadian lottery telemarketers Win USA Services Ltd., the FTC charged the defendant with violating the FTC Act and the Telemarketing Sales Rule by

providing "substantial assistance and support" to Canadian telemarketers, including the Win USA defendants. The FTC alleged that Cordeiro provided account debiting services to process demand drafts through U.S. banks, and that he knew, or should have known, that the telemarketing schemes were fraudulent and violated federal law. Cordeiro agreed to a consent order barring him from providing substantial assistance or support, including but not limited to customer payment processing services, to anyone who offers or promotes foreign lottery sales to U.S. citizens.

- Press Release (Complaint and Final Order): http:/www.ftc.gov/opa/2001/02/win2.htm

- *FTC v. Farpoint Services Inc. et al. [American Card Services]*, C01-1593P (W.D. Wash., civil complaint filed Oct. 9, 2001, stipulated final judgment entered Sept. 9, 2002).

  In a civil action related to *United States v. Arcand and Galway* (see above), the FTC charged two Canadian citizens and five corporations (incorporated in the United States, Canada, and other foreign jurisdictions) with violating the FTC Act and the Telemarketing Sales Rule by inducing consumers into paying as much as $299 for one of two worthless credit card "protection" packages. The FTC also charged that the defendants used merchant accounts established in their names to launder credit card purchase for unrelated sellers lottery tickets, British bonds, and consumer benefits packages. In September 2002, the FTC entered into a stipulated final order with the defendants that bans them from telemarketing credit card loss-protection packages and from credit card laundering. The order also bars them from making misrepresentations similar to those alleged in the complaint and from disclosing their consumer lists to anyone besides the FTC or other enforcement agencies. The order imposes a judgment for $3.3 million, with all but $436,000 suspended due to the defendants' inability to pay. To date, the defendants have paid $100,000 of this judgment.

  - Press Release (Stipulated Permanent Injunction and Final Judgment): www.ftc.gov/opa/2002/10/americancard.htm

- Press Release (Complaint): http://www.ftc.gov/opa/2001/10/ditch.htm

- *FTC v. Icon America, Inc.*, No.: 2:01-CV-320 (D. Vt., civil complaint filed Oct. 2001, stipulated final judgment filed Jan. 28, 2003)

  The FTC filed this civil action in October 2001 against two individual defendants, based in Canada, and two Canadian corporations. The FTC charged that the defendants used telemarketing to sell credit card loss protection to consumers for prices ranging from $299 to $369. Using scare tactics, the defendants allegedly claimed that consumers' credit card numbers were available on the Internet and accessible to criminals, and that the consumers would be held liable for any unauthorized charges, if anyone gained access to this information. The complaint stated that Icon representatives told consumers that the company's loss protection services would cover any unauthorized charges due to such theft. The FTC entered into a settlement with the defendants in January 2003, which bars the principals from making the types of misrepresentations alleged in the complaint, violating the Telemarketing Sales Rule, and selling or transferring their customer lists. The order also contains a suspended judgment for $1.5 million, the amount of Icon's gross sales and the approximate amount of consumer injury, and requires the defendants to pay $25,000 that the Commission may use for consumer redress.

  - Press Release (Complaint): http://www.ftc.gov/opa/2001/10/ditch.htm
  - Press Release (Stipulated Final Judgment): http://www.ftc.gov/opa/2003/01/icon.htm

- *FTC v. Opco International Agencies et al.*, No. C01-2053R (W.D. Wash., civil complaint filed Feb. 21, 2001, default judgment entered Dec. 28, 2001) [Emptor]

  After an investigation coordinated with the British Columbia Ministry of Attorney General, the Federal Bureau of Investigation, and the Royal Canadian Mounted Police through Project Emptor [see *United States v. Wilson*, below], the FTC filed a civil complaint against three individual defendants and eight affiliate corporate defendants for a scheme designed

to defraud consumers through the sale of credit card "protection" insurance and "debt consolidation" programs. Most of the corporate defendants were either based or operated from British Columbia. The British Columbia Ministry of Attorney General filed a coordinated civil action and obtained a freeze on Canadian defendants' assets.

On December 28, 2001, the U.S. district court entered a default judgment banning the defendants from engaging in any credit card protection or debt consolidation businesses, prohibiting them from making misrepresentations in violation of the FTC Act and the Telemarketing Sales Rule. The court also held the defendants jointly and severally liable for monetary equitable relief for consumer redress in the amount of $5.5 million.

- Press Release (Complaint and TRO): http://www.ftc.gov/opa/2001/02/opco.htm

- *FTC v. R&R Consultants, Inc. et al.*, 01-CV-1537 TJM (N.D.N.Y., civil complaint filed Oct. 10, 2001, stipulated final judgment entered Apr. 25, 2002); *State v. R&R Consultants* (Cole Co. Circuit Ct., Mo., civil action filed April 2001)

In this civil action, the FTC charged a Montreal-based telemarketer, Reuben Ross, and a company, R&R Consultants, with violating the FTC Act by allegedly employing a variation on more traditional credit-card loss-protection schemes. R&R allegedly falsely promised to remove all of the consumer's personal information from the Internet, thus protecting them from identity theft. According to the civil complaint, the defendants told consumers that their personal information, including credit card numbers, was available on the Internet and that they faced unlimited liability if it was obtained by crooks. The defendants allegedly promised to remove all consumers' personal information from the Internet and to remove consumers' names from all telemarketing lists. In addition, for an advance fee of several hundred dollars, consumers were allegedly told that they would receive a low-interest credit card, but only received a list of banks and a booklet of tips on how to obtain a credit card.

In April, 2002, the FTC entered into a settlement with Ross, individually and as an officer of R&R Consultants and its affiliated companies. The court order bans the defendants from marketing both "credit-related goods or services" and "protection services" through any form of sales activity, including telemarketing, direct mail, and Internet marketing. It also prohibits defendants from a engaging in a number of specific marketing abuses at issue in the case. Finally, the order required defendants to pay $111, 354 in consumer redress.

Another civil action, brought by the Missouri Attorney General, charged that Ross and R&R Consultants marketed a phony international "do-not-call" list. According to the Attorney General, the defendants falsely told consumers that, for a $289 fee, their names would be removed from an international telephone and mail solicitation database. In addition, the defendants allegedly falsely told consumers they would be protected from fraudulent credit card charges. The Attorney General subsequently obtained an order permanently barring the defendants from making misrepresentations and requiring the payment of $7,440 in investigatory costs and $7,060 in restitution.

In a related action, the North Carolina Attorney General filed suit against R & R Consultants and Ross. The Attorney General alleges that the defendants falsely told consumers they provided credit card security and identity theft services for VISA. In addition, the defendants falsely promised consumers a credit card for $25. Attorney General Cooper further alleges that the defendants marketed their "peace and quiet" program and, after being turned down, charged consumers anyway. The lawsuit seeks reimbursement to consumers, a permanent injunction, and civil penalties of up to $25,000.

- Press Release (FTC Complaint): http://www.ftc.gov/opa/2001/10/ditch.htm
- Press Release (Stipulated Judgment and Order for Permanent Injunction): http://www.ftc.gov/opa/2002/04/rrconsultants.htm
- Press Release (Missouri Order): http://www.ago.state.mo.us/091801b.htm

- *State v. Alini International Marketing, Inc., Telehub-Link Corp. (operating as Triple Gold Benefits), and 3557561 Canada Inc. (operating as Platinum 2000, Continental Benefits Group and the Alliance for Family Security)* (N.Y. Sup. Ct., complaints announced April 20, 2001)

  In these civil actions, brought by the New York State Attorney General, three Montreal-based companies were charged with engaging in deceptive, fraudulent and illegal business practices. Hundreds of consumers across New York and other states complained that the companies deceived them into paying approximately $200 in advance for an all-purpose credit card such as a Visa or MasterCard. Instead of providing the promised credit cards, these companies sent consumers so-called "financial benefits" packages which were of little or no interest to the consumers. Many consumers received nothing at all for their payment, but hundreds of consumers lost approximately $5 million US.[128] In October 2001, the New York State Supreme Court ordered Telehublink Corp. and 3557561 Canada Inc. to cease doing business in the state unless they post $500,000 bonds.[129]

  - Press Release (Complaints): http://www.oag.state.ny.us/press/2001/apr/apr20b_01.html

- *State v. World Wide Source Publishing, Inc. et al*. (Chittenden Super. Ct., Vt., civil action filed November 2001)

  This civil action, brought by the Vermont Attorney General, charged World Wide Source Publishing, Inc. (WWS) and five of its officers with violating the Vermont Consumer Fraud Act in the course of selling listings in a directory called the "American Business Index." According to the Attorney General''s complaint, WWS, using a Vermont return address, solicited orders for two-year listings in its directory for $399.95, by means of outbound telemarketing calls to businesses throughout the United

---

[128] *See* PhoneBusters, News Release (April 21, 2001) (reprinting article from Montrealgazette.com), http://www.PhoneBusters.com/Eng/Charges_Arrests/April_21_2001_1a.html.

[129] *See* PhoneBusters, News Release (October 11, 2001) (reprinting article from CBC), http://www.PhoneBusters.com/Eng/Charges_Arrests/October_11_2001_1a.html.

States. The civil complaint alleged that WWS, among other things, had made various misrepresentations to customers and had billed many customers without their authorization.

On March 21, 2002, the Attorney General announced that WWS and Ameri-Source Publications, Inc. (a company which shares common management and ownership with WWS and uses a return address in New York State) would together pay a total of $125,000 to the State of Vermont and provide refunds to all of their Vermont customers. The settlement also bars the defendants from doing business in or into Vermont, or using a business address or facilities in the state.

- Press Release (Settlement): http://www.state.vt.us/atg/press03212002.htm

- Civil and Administrative Actions - Internet Fraud

  - *FTC v. 1268957 Ontario, Inc. dba National Domain Registry et al.*, 01-CV-0243 (N.D. Ga., civil complaint filed February 12, 2001, stipulated final order entered Mar. 29, 2002)

    In this civil action, the FTC filed a civil complaint against two Canadian corporations and one individual Canadian defendant who ran an Internet domain name scheme that duped consumers into needlessly registering variations of their existing domain names by deceptively contending that a third party, acting in bad faith, was about to claim it. According to the FTC's complaint, no third party had applied for the name, and the information disseminated by defendants was false, in violation of the FTC Act and the Telemarketing Sales Rule.

    At the agency's request, a U.S. District Court issued a temporary restraining order, froze the defendants' assets, and shut down their Web sites, pending trial. In March 2002, the defendants agreed to pay $375,000 in consumer redress to settle the FTC's charges. The settlement also barred the defendants from making false or misleading statements in the sale of goods or services related to domain names, e-mail or Web-hosting services; barred them from using unsolicited faxes for marketing; and barred them from violations of the Telemarketing Sales Rule.

- Press Release (Complaint and Temporary Restraining Order): http://www.ftc.gov/opa/2001/02/morgenstern.htm
- Press Release (Stipulated Final Order for Permanent Injunction and Consumer Redress): http://www.ftc.gov/opa/2002/04/morgenstern.htm

2000

- Criminal Prosecutions - Internet Fraud

  - *Regina v. Friskie* (Saskatchewan Provincial Court, charges laid 2000)/*FTC v. Skybiz.com, Inc. et al.*, Civil Action No. 01-CV-0396-EA (N.D. Okla., complaint filed May 30, 2001)

    In 2000 and 2001, law enforcement and regulatory agencies around the world, including Canada and the United States, brought a series of related criminal and civil actions against SkyBiz.com. Skybiz purported to sell online tutorials on Web-based products, using website presentations, in-person sales presentations, seminars, teleconferences, and other marketing material, to tout the opportunity to earn thousands of dollars a week by recruiting new "Associates" into the program.[130] Authorities, however, charged that SkyBiz was an illegal pyramid scheme.

    In May 2000, a SkyBiz associate, Jeanette Friskie, was charged in Saskatchewan with operating a pyramid scheme.[131] On September 24, 2001, the Provincial Court of Saskatchewan determined that SkyBiz was a pyramid scheme, found Friskie guilty of running an Internet-based pyramid scheme, and fined her CA $20,000.[132]

---

[130] *See* FTC, Press Release (June 18, 2001), http://www.ftc.gov/opa/2001/06/sky.htm.

[131] *See* Lori Enos, EcommerceTimes.com, *U.S. Files Charges over $175M Online Pyramid Scheme*, NewsFactor.com, June 19, 2001, http://www.newsfactor.com/perl/story/11346.html.

[132] *See* R. v. Friskie, [2001] S.J. No. 565, Information No. 24021184 (Saskatchewan Provincial Court, Sept. 24, 2001); Law Society of Saskatchewan, News Archives 2001,

In a related civil proceeding, in May 2001, the FTC filed a civil action in U.S. District Court in Tulsa, Oklahoma, against six individuals and four corporations including SkyBiz.com. The FTC charged that the SkyBiz.com scheme may have defrauded consumers of approximately $175,000,000 worldwide. At the request of the FTC, the District Court halted all unlawful activities of the SkyBiz operation, froze the defendants' assets to preserve them for consumer redress, appointed a receiver,[133] and later ordered the return of assets, including tens of millions in an account in Ireland, to the United States, for possible use as consumer redress. Ultimately, in January 2003, the FTC reached a settlement with nine of the ten defendants shortly before trial that would provide US $20 million for consumer redress. (Distribution of this redress fund will begin in the near future.) The settlement also barred all of the defendants from participating in pyramid schemes or misrepresenting the amount of sales, income, profits or rewards of any future business venture. The tenth defendant also settled prior to trial in April 2003.[134] The FTC received substantial assistance from the RCMP and other international consumer protection law enforcement bodies, including the Australian Competition and Consumer Commission, the South African Department of Trade and Industry, the New Zealand Commerce Commission, and the United Kingdom Department of Trade and Industry.

- Criminal Prosecutions - Telemarketing Fraud

  - *Regina v. Tagheri et al.* (Ontario Superior Court, charges laid 2000) [Toronto Strategic Partnership]

    On June 7, 2000, the Strategic Partnership and Peel Regional Police searched a company operating as Britania Group, and discovered four others called Barnes & Associates, Renforth Group, Highland

---

http://www.lawsociety.sk.ca/newlook/archive/Archive01Dec.htm.

[133] *See* FTC, Press Release (June 18, 2001), http://www.ftc.gov/opa/2001/06/sky.htm.

[134] *See* FTC, Press Release (March 24, 2003; corrected Apr. 1, 2003), http://www.ftc.gov/opa/2003/03/skybiz.htm.

International, and Stratford International. The companies allegedly offered loans to U.S. citizens for an advanced fee. They led victims to believe that their offices were in U.S. states including New York, while they were actually operating out of an industrial office space in Peel Region. The fees received were forwarded across the United States to Winnipeg, Newfoundland, and Vancouver before being returned to a Toronto mail facility. The companies were shut down and six persons were arrested. Approximately CA $46,281 was seized and returned to consumers. The RCMP Commercial Crime Units in Winnipeg, Vancouver and Quebec and the Newfoundland Royal Constabulary provided valuable assistance to the Partnership in the matter.

One of the persons arrested and charged in June 2000, Omid Taghavi, continued to operate, and was further charged with Breach of Recognizance. On March 27, 2002, Omid Taghavi pleaded guilty to fraud over $5,000. He was sentenced to 1-1/2 years conditional and 2 years probation, and ordered to pay $18,000 in restitution. On April 5, 2002, another accused, Charlene Charlton, appeared in court on a charge of fraud over $5,000. She paid $500 restitution and provided the court with a letter of apology to the American people and the FTC, which resulted in the Crown withdrawing the charge. On May 17, 2002, a third accused in the case, Jamie Strawn, pleaded guilty under the Loan Brokers Act and paid $1,000.00 in restitution. Strawn is required to pay a total of $7,500.00 in restitution and was to be on probation for a period of 1 year with conditions. Once all restitution has been paid, the Criminal Code charge of Fraud Over $5,000.00 will be withdrawn.

- *United States v. Babuin*, No. 00-2776M (C.D. Cal., criminal complaint filed November 13, 2000) [Emptor]

  This criminal case, brought by the United States Attorney's Office in Los Angeles, began with a criminal complaint charging one defendant (Timothy Babuin) with fraud-related offenses pertaining to his alleged role in a Vancouver telemarketing company, NAGG Holdings. NAGG Holdings allegedly sold bogus lottery tickets and bogus savings bonds to U.S. and Canadian victims. Babuin has now signed a plea agreement under which he would waive extradition, plead guilty, and receive a

sentence of six years imprisonment plus forfeiture of approximately $2 million in assets.

- Congressional Testimony (2001): http://govt-aff.senate.gov/061501_warlow.htm

- *United States v. Cartagena*, No. CR 00-613 (C.D. Cal., indictment filed June 8, 2000) [Emptor]

  This criminal case, brought by the United States Attorney's Office in Los Angeles, charged one defendant (Eduardo Cartagena) with fraud-related offenses pertaining to a lottery and "rip-and-tear" scheme. Cartagena, had managed boiler rooms in Burnaby, British Columbia, that were part of an operation called, at various times, Global Dividends International, Horizon 2000 Investments International, and Platinum International. The day after Cartagena's arrest in Blaine, Washington, on May 9, 2000, RCMP officers, in cooperation with the British Columbia Ministry of the Attorney General and the FBI, conducted searches at two telemarketing boiler rooms in Burnaby, under the provisions of the British Columbia Trade Practice Act.

  At trial, Cartagena was convicted on November 24, 2000 on 10 counts of wire fraud. The testimony at trial showed that the business name was changed often to avoid detection of the scheme. Cartagena's stepfather and mother, Jacques and Christina Tanguay (see above), owned the operation and also operated a boiler room in Québec. On May 14, 2001, Cartagena was sentenced to 70 months imprisonment and restitution to victims. The sentence was based in part on the jury's specific finding that Cartagena had defrauded at least 10 victims over the age of 55, which made him eligible for an increased sentence under the telemarketing fraud enhancement provisions of 18 U.S.C. § 2326.

  - Press Release (Conviction): http://www.usdoj.gov/usao/cac/pr/pr2000/209.htm
  - Congressional Testimony (2001): http://govt-aff.senate.gov/061501_warlow.htm

- *United States v. Descent*, No. 8:00-CR-186-T-30TBM (M.D. Fla., indictment filed June 19, 2000)

  This criminal case, brought by the United States Attorney's Office in Tampa, charged Serges Jacques Descent in a 57-count indictment with conspiracy, mail fraud, money laundering conspiracy, and money laundering (18 U.S.C. §§ 1956 and 1957), including the telemarketing fraud enhancement under 18 U.S.C. §§ 2326(5). On January 17, 2001, a federal jury returned a verdict of guilty against Descent on all counts of the indictment. According to the evidence at trial, in 1998 and 1999 Descent used bank accounts in St. Petersburg, Florida and Canada to channel funds from victims' checks that were sent in response to calls from a lottery room, presumed to be in Canada. Victims named in the indictment included 13 people in their 70s and 80s, and four of those victims were so frail that they could not travel to testify at trial and had their testimony taken by video deposition. Descent was scheduled for sentencing on July 20, 2001. A second defendant, Vasilis Kolitsidas, was a fugitive in this case, but was arrested in Montreal in February, 2001 in connection with the Denis Morin arrest (see above).

  - Congressional Testimony (2001): http://govt-aff.senate.gov/061501_warlow.htm

- *United States v. Ghirra*, (C.D. Cal., criminal complaint filed February 7, 2000) [Emptor]

  This criminal case, brought by the United States Attorney's Office in Los Angeles, charged a Vancouver, British Columbia resident (Michael Ghirra) with wire fraud and mailing lottery communications. Ghirra was allegedly the owner and operator of WIN USA (a/k/a International Registration Australian Lottery (IRAL), International Canadian Lottery System, and Ipex Services Ltd.) from approximately April 1997 through November 1998. Ghirra allegedly had obtained approximately $5 million from his lottery operations. Ghirra had previously been a defendant in a civil action filed by the FTC on November 7, 1998 concerning his activities with WIN USA and IRAL. The FTC action was conducted with the cooperation of the Royal Canadian Mounted Police and the British Columbia Ministry of Attorney General, which filed suit against the same

defendants in a British Columbia court. That court issued an asset freeze and appointed a receiver, pending trial.

The FTC civil action resulted in the granting of the FTC's motion for summary judgment on April 13, 2000. The summary judgment barred the defendants from selling tickets, chances, interests or registrations in any lottery to U.S. residents and from selling any product or service to U.S. residents in a manner that violates the FTC Act, the Telemarketing Sales Rule, or the Arizona and Washington consumer protection statutes. In addition, the court required that the defendants pay $3,189,373 in consumer redress. Ultimately, the parties agreed to payment of $500,000, which represented all of the available funds frozen by the British Columbia Ministry of Attorney General in the concurrent law enforcement action in Canada.

- Complaint (FTC): http://www.ftc.gov/os/1998/9811/winusacomp.htm
- Congressional Testimony (2001): http://govt-aff.senate.gov/061501_warlow.htm
- Press Release (FTC): http://www.ftc.gov/opa/2001/02/win2.htm

- *United States v. Guerrero* (W.D. La., indictment filed November 15, 2000)

This criminal case, brought by the United States Attorney's Office in Western Louisiana, charged a resident of British Columbia (Nelson Guerrero) on six counts of conspiracy, wire fraud, and money laundering. Guerrero and others allegedly operated a fraudulent telemarketing business in Canada that telephoned victims and promised them a substantial cash prize if they sent payments to cover "taxes" and to convert Canadian currency to U.S. dollars. Guerrero also allegedly used the aliases Nelson Ramirez, Alex Roberto, and Anthony Miranda.

- Congressional Testimony (2001): http://govt-aff.senate.gov/061501_warlow.htm

- *United States v. Marc Wilson*, No. SA 00-172M (C.D. Cal., criminal complaint filed June 13, 2000)

  This criminal case, brought by the United States Attorney's Office in Los Angeles, charged one defendant (Marc Wilson) with mail, wire, financial institution, and credit-card fraud, pertaining to an alleged credit-card protection scheme. Wilson, doing business as OPCO International Inc. and related companies, as well as American Fraud Watch Services, Inc., allegedly operated a fraudulent telemarketing scheme in which U.S. residents were telephonically contacted from Canada in an effort to have those residents disclose their Visa and/or MasterCard numbers to the callers. Those numbers were then billed without authorization for $299.00 each. In February 2000, the OPCO executive offices were searched and computers and other documentation were seized. As described above [see FTC v. OPCO], the FTC and the British Columbia Director of Trade Practices also filed simultaneous civil actions against both individuals and the companies, seeking US $4.5 million in consumer redress. The United States intends to seek Wilson's extradition from Canada.

  - Congressional Testimony (2001): http://govt-aff.senate.gov/061501_warlow.htm

- Civil and Administrative Enforcement Actions - Telemarketing Fraud

  - *FTC v. B.B.M. Inv., Inc.*, No. C00-0062 (W.D. Wash., civil complaint filed Jan. 13, 2000, proposed stipulated final order filed September 18, 2001) [Emptor]

    In this civil action, the FTC charged a Vancouver-based telemarketer with making deceptive representations to U.S. consumers in connection with the sale of bogus bonds and bond pool shares that also had a lottery contest feature. Canadian authorities brought proceedings against the same defendant in British Columbia. In both proceedings, defendants were temporarily barred from selling the bonds and assets were frozen.

    A stipulated final judgment was filed in the U.S. action on September 18, 2001. The stipulation bars defendants from marketing any lottery-related goods or services and from making certain representations in connection

with the legitimate sale of government securities. It also bars the defendants from distributing their customer lists.

- Press Release (Complaint): http://www.ftc.gov/opa/2000/01/bbm.htm
- Press Release (Stipulated Final Judgment): http://www.ftc.gov/opa/2001/09/bbm2.htm

- *FTC v. Canada Prepaid Legal Services, Inc.*, No. CV00-2080Z (W.D. Wash., civil complaint filed Dec. 11, 2000) [Emptor]

In civil actions related to *United States v. Babuin* (see above), in December 2000, the FTC and Canadian law enforcers filed civil actions against Timothy Babuin and 13 other corporate and individual defendants, alleging that their activities in connection with the sale of bogus bonds and bond pool shares with a lottery contest feature violated the FTC Act and the FTC's Telemarketing Sales Rule (TSR). The defendants misrepresented that consumers would receive payments by purchasing bonds; misrepresented that consumers agreed to buy bonds and owed the defendants money; unfairly charged some consumers whom they never contacted; and failed to disclose to consumers that the sale of the bonds is a crime. Alleged violations of the TSR included making false or misleading statements about the "cash awards"; falsely claiming that consumers' credit cards would not be charged without authorization; and failing to disclose that sale of the bonds is a federal crime. In addition, the agency charged a number of the defendants with assisting deceptive telemarketers to violate the law by providing them with access to their merchant accounts for processing credit card charges.

After RCMP and British Columbia Attorney General representatives executed a search on the premises of NAGG on December 13, 2000, the Attorney General of British Columbia initiated a parallel enforcement action and asset freeze in the Province of British Columbia, Canada. The FTC also obtained an asset freeze in U.S. District Court in Seattle. Under the British Columbia Trade Practices Act, approximately CA $13 million in assets have been frozen. In December 2002 the FTC announced a stipulated final judgment and order, filed with the U.S. District Court for the Western District of Washington. The settlement requires defendants

to release all claims to approximately $1 million frozen by the British Columbia Solicitor General, with almost the entire amount to be returned to the U.S. for consumer redress. The defendants are barred from participating in future lottery schemes against U.S. consumers, including bond programs with a lottery feature. They are also barred from making unauthorized charges against consumers' credit card accounts, from making misrepresentations, and from disclosing consumers' credit card information to others.

- Press Release (Civil Action): http://www.ftc.gov/opa/2000/12/nagg.htm
- Press Release (Stipulated Final Judgment): http://www.ftc.gov/opa/2002/12/nagg.htm

- *FTC v. Growth Plus Int'l*, No. 00C 07886 (N.D. Ill, civil complaint filed Dec. 18, 2000, default judgment entered April 16, 2002)

  In this civil action, the FTC charged Canadian telemarketers with targeting elderly consumers, inducing them to buy shares in a Canadian lottery ticket or series of tickets at prices ranging from $39 to almost $600. The telemarketers allegedly misrepresented both the legality of purchasing foreign lottery tickets in the U.S. and the consumers' chances of winning the lottery. The Court entered a final judgment barring the telemarketing claims and ordering restitution in the sum of $4.2 million.

  - Press Release (Complaint): http://www.ftc.gov/opa/2000/12/gains2.htm
  - Press Release (Stipulated Final Judgment): http://www.ftc.gov/opa/2002/06/crossbordercaselist.htm

- *FTC v. TSI Financial Servs.*, No.: 00-CV-906 (W.D.N.Y., civil complaint filed Oct. 23, 2000) [Toronto Strategic Partnership]

  In this civil action, the FTC charged T.S.I. Financial Services of Ontario, Canada with running a bogus credit-card loss-protection scam. The FTC alleged that the defendants (1) misrepresented their identity to consumers; (2) misrepresented consumers' liability for unauthorized credit card charges; and (3) posted unauthorized charges to consumers' credit card

accounts. The court entered a permanent injunction and ordered the defendants to make restitution in the sum of $ 4.857 million.

- Press Release (Complaint): http://www.ftc.gov/opa/2000/10/protectdecpt.htm
- Press Release (Order): http://www.ftc.gov/opa/2002/06/crossbordercaselist.htm

- *United States v. Fry* (INS/U.S. Court of Appeals for Ninth Circuit, 2003)

In June 2000, the United States Immigration and Naturalization Service began proceedings to deport John William Fry, a Canadian citizen, for having been convicted of an aggravated felony. Fry had been a salesperson at Legendary Concepts, a telemarketing boiler room in Las Vegas, and participated in fraudulent telemarketing. In 1997, Fry was convicted of multiple fraud-related charges in federal court, and was later sentenced to 46 months imprisonment and restitution of $1,928,911. On March 18, 2003, the United States Court of Appeals for the Ninth Circuit upheld a denial of Fry's petition for habeas corpus relief. It rejected Fry's argument that his trial counsel gave him ineffective assistance by not telling him that he could be deported if convicted.[135]

1999

- Arrests and Search Warrants

  - *Loan Consolidation Services Case (Ontario)*

On March 3, 1999, members of the Toronto Police Fraud Squad, with the assistance of the Ontario Ministry of Consumer and Commercial Relations, RCMP, and PhoneBusters, executed search warrants in the Toronto area closing loan companies (offering loan consolidation services) known as Millennium Group and Elite Insurance. Seven persons were arrested for fraud over $5,000.

---

[135] *See United States v. Fry*, 322 F.3d 1198 (9th Cir. 2003).

- Criminal Prosecutions - Telemarketing Fraud

  - *Regina v. Allen et al.* (Ontario Super. Ct., charges laid April 1999)

    This criminal case, brought by the Crown Law Office (Criminal) in Brampton, Ontario, charged three telemarketers in Mississauga, Ontario (William B. Allen, Sonia Lam, and Zorino Ostroman) with defrauding the public for their alleged roles in a lottery scheme that targeted mostly senior citizens.

  - *Regina v. Card and Sanders* (Ontario Super. Ct., charges laid 1999)

    In March 1999, a search warrant was executed on a loan broker operation advertising in U.S. newspapers in the name of Goodlife as well as six other names. The search resulted in the arrest of 10 individuals who were charged with fraud. On November 29, 2000, seven of the defendants pleaded guilty to charges under the Ontario Loan Brokers Act and agreed to pay restitution in the amount of $1,700. Another defendant, a young offender, had previously pleaded guilty and was put on probation. The remaining two defendants, Kevin Bryan Card and Bennie Sanders, were remanded for trial on the fraud charges.

    On December 14, 2001, Card and Sanders were convicted of Fraud Over $5,000.00 and Possession Under $5,000.00 after a seven-day trial at Scarborough Court. The FTC arranged and paid for three American victims of the scheme to attend court and give testimony. Card was sentenced to serve a one-year conditional sentence with a large number of conditions, two years probation, $10,000 restitution, and 240 community service hours. On January 28, 2002, Sanders was sentenced to serve a one-year conditional sentence with a large number of conditions, two years probation, $10,000.00 restitution, and 120 community service hours.

- *United States v. Gilham and Pomerantz*, (C.D. Cal., indictment filed December 1999)

  This criminal case, brought by the United States Attorney's Office in Los Angeles, began with the arrest of two Montreal telemarketers (George R. Gilham and Lisa A. Pomerantz) in Los Angeles on November 17, 1999. Both defendants reportedly drove from Montreal to Los Angeles in order to pick up $140,000 in cash from an elderly victim and give her a counterfeit $5.5 million check, purportedly for "lottery winnings." After being indicted in December 1999 on mail fraud and related charges, both defendants pleaded guilty to fraud-related charges in January 2000. On May 22, 2000, Gilham and Pomerantz were sentenced to 30 months and 27 months imprisonment, respectively.

- Civil and Administrative Enforcement Actions

  - *FTC v. NCCP Ltd. dba National Credit Card Protection Ltd*, Civ. A. No. 99-CV-0501 A(Sc) (W.D.N.Y., civil complaint filed July 22, 1999, stipulated final judgment entered July 23, 1999).

    In the FTC's first Y2K-related fraud case, Toronto-based credit card protection marketers agreed to pay $100,000 to settle FTC charges of misrepresenting their protection program, including protection against potential Y2K-related problems. Defendants agreed to be permanently banned from engaging in the credit card protection and credit card registration business.

    - Press Release (Complaint and Order): http://www.ftc.gov/opa/1999/07/nccp.htm

1998

- Arrests and Search Warrants - Telemarketing Fraud

  - *Loan Consolidation Services Cases (Ontario)*

    On July 16, 1998, members of the Toronto Police Fraud Squad, with the assistance of U.S. Postal Inspectors, executed search warrants in the Toronto area, two men – Donald Hugh and Sherif Scott, of Toronto – were arrested in fraud charges, and six telemarketing companies (offering loan consolidation services) were closed.

    On June 23, 1998, the Toronto Police Service and the Ontario Ministry of Consumer and Commercial Relations, with the assistance of other law enforcement agencies, executed 27 search warrants on telemarketing boiler rooms and associated addresses. The rooms allegedly operated as 40 companies in the Toronto area, advertising in the United States as loan consolidation services. Two persons were charged with fraud over $5,000.

- Criminal Prosecutions - Telemarketing Fraud

  - *Regina v. American Family Publishers, Publishers Central, and First Canadian Publishers and Sharma* (Quebec Super. Ct., charges laid ca. 1998)

    This criminal case, brought by the Competition Bureau of Industry Canada in Quebec, charged corporate entities operating under the names American Family Publishers, Publishers Central, and First Canadian Publishers, and the company's president, Vijay Sharma, with violating the misleading advertising provisions of the Competition Act. On March 5, 1999, the defendants pleaded guilty to the charges. On May 5, 1999, the Quebec Superior Court imposed a $1 million fine against the corporate entities, and a $100,000 fine against Sharma. The sentence was the highest ever imposed against a deceptive telemarketing operation under these provisions of the Act. Previously, on March 11, 1999, the Court sentenced four other telemarketers to jail terms ranging from two to six months and 20 to 120 hours of community service. One additional telemarketer who pleaded guilty was fined $5,000, and a second additional telemarketer who pleaded guilty was to be sentenced in June 1999.

- Press Release (Sentence): http://strategis.ic.gc.ca/SSG/ct01521e.html

- *Regina v. Nichols* (Ontario Super. Ct., sentenced 1998)

  On April 8, 1999, a judge in Toronto, Ontario sentenced Reed Nichols, a telemarketer who purported to sell packages of lottery tickets, to 5 years and three months' service in the penitentiary. During the course of his scheme, Nichols had persuaded an 84-year-old woman living in Chicago to give him $1,005,000. In his opinion, the judge made clear that he would have sentenced Nichols to a seven-year term of imprisonment had Nichols not returned the balance of the funds, approximately $772,000, to the victim.

- *Regina v. Obront* (Ontario Super. Ct., pleaded guilty July 3, 1998)

  On July 3, 1998, Alan Obront, who controlled a fraudulent gemstone telemarketing operation known as Royal International Collectibles (RIC), and three other telemarketers pleaded guilty to one count of defrauding the public. Over a 10-year period, according to one account, RIC earned $50 million. On or about July 7, 1998, a judge in Toronto, Ontario sentenced Obront to four years' imprisonment.

- Civil and Administrative Enforcement Actions

  - Commonwealth of Pennsylvania v. Systems 3 Marketing (M.D. Penn., filed Dec. 14, 1998) [Emptor]

    In December 1998, the British Columbia Ministry of Attorney General filed a civil action in British Columbia, and the Pennsylvania Attorney General filed a parallel civil action in federal court in central Pennsylvania, against Vancouver-based telemarketers selling bogus foreign lottery chances to U.S. victims. In April 1999, the FTC intervened in the Pennsylvania case to ensure that the court would order nationwide redress for injured consumers. In June 1999, the Pennsylvania court entered a summary judgment in favor of Pennsylvania and the FTC and awarded redress of $2.4 million (uncollected). The U.S. DOJ Office of Foreign Litigation initiated proceedings in British Columbia to attempt to collect. Defendants were also barred from engaging in any form of telemarketing,

trade or commerce in Pennsylvania, and from marketing foreign lottery schemes to U.S. residents.

- Press Release (Order): http://www.attorneygeneral.gov/press/release.cfm?p=42E56C28-E948-11D3-8DEA0060972D2515

- *FTC v. Pacific Rim Pools International*, C97-1748R (W.D. Wash, civil complaint filed Nov.1997, proposed order for permanent injunction and final judgment filed Dec. 11, 1998), and *FTC v. Woofter Investment Corp., d.b.a. ATMS*, CV-S-97-005150LDG (RLH) (D. Nev., civil complaint filed Apr. 1997, stipulated order for permanent injunction and final judgment filed Dec. 15, 1998).

  These related cases were the FTC's first multi-agency enforcement effort against Canadian firms targeting U.S. residents for telemarketing schemes, and involved the FTC's first use of the credit card laundering rule under the Telemarketing Sales Rule. Pacific Rim/Pools was a Vancouver-based telemarketer making deceptive representations in connection with sale of lottery tickets and chances to U.S. consumers. ATMS was a Las Vegas-based firm that processed credit card charges for more than 50 Canadian lottery telemarketers. The FTC proceeded against ATMS in Nevada and against Pacific Rim Pools in Washington State, in cooperation with the British Columbia Ministry of Attorney General and the Washington Attorney General's Office. Both targets ceased operations as a result of settlements in late 1998. Funds totaling $1.38 million (U.S.) were distributed to U.S. consumers.

  - Press Release: (Settlements): www.ftc.gov/opa/1999/9901/poolswoof.htm
  - Press Release (Complaint): www.ftc.gov/os/1997/9704/comp6.htm

- *FTC v. Walton, dba Pinnacle Financial Servs.*, CIV98-0018 PCT SMM (D. Ariz., civil complaint filed Jan. 6, 1998, stipulated final judgment filed June 2, 1998)

  Defendant Gary Walton, dba Pinnacle Financial Services, served as a "turndown room" for several fraudulent Canadian advance fee loan telemarketers, including Allied Credit referral Service, operating from Richmond , British Columbia. Walton also operated his own advance fee loan scheme. In January 1998, the FTC proceeded against Walton and the British Columbia Ministry of Attorney General issued a cease and desist order against Allied and obtained court orders authorizing the seizure and return of checks sent in by victims. Defendants ceased operations as a result of the FTC settlement with Walton and the British Columbia settlement with Allied in June 1998. Uncashed checks and money orders worth $50,000, seized when Allied was shut down in January, were returned to U.S. consumers in July 1998.

  - Press Release (Settlements): www.ftc.gov/opa/1998/07/retchek.htm; http://www.ftc.gov/opa/1998/06/pinnacle.htm

- *FTC v. Windermere Big Win Int'l,* Case No. 1:98cv08066 (N.D. Ill., civil complaint filed Dec. 16, 1998, final order issued Aug. 17, 2000)

  In 1998, the FTC filed a civil complaint against five individuals and three corporations who induced elderly consumers to buy shares in a Canadian lottery ticket or series of tickets at prices ranging from $39 to almost $600. The FTC charged that the telemarketers violated the FTC Act and the Telemarketing Sales Rule by falsely claiming that it was legal to buy and sell foreign lottery tickets, failing to disclose to consumers that the sale of, and trafficking in foreign lotteries is a crime in the United States, and making other false statements to induce consumers to buy the tickets. The U.S. District Court issued a permanent injunction prohibiting deceptive claims and ordering $19.7 million in restitution to victims. The U.S. Department of Justice's Office of Foreign Litigation filed a parallel civil action in Canada, and was able to have the restitutionary provisions of the

U.S. district court's judgment enforced by the Ontario Superior Court of Justice and affirmed by the Court of Appeal.[136]

- Press Release (Complaint): http://www.ftc.gov/opa/1999/09/wind.htm
- Press Release (Order): http://www.ftc.gov/opa/2000/10/windermere.htm

- *FTC et al. v. Win USA Servs. et al.*, Civil Action No. C98-1614Z (W.D. Wash., civil complaint filed Nov. 1998, final order issued Feb. 5, 2001)

  In this civil action, the FTC, along with the Attorneys General of Arizona and Washington, charged Vancouver-based telemarketers with making deceptive representations in connection with the sale of lottery tickets and chances to U.S. consumers. The investigation was conducted with the cooperation of the RCMP and B.C. Ministry of Attorney General, which filed suit against the same defendants in a British Columbia court, obtaining an asset freeze and the appointment of a receiver. In April 2000, the U.S. District Court entered summary judgment, barring defendants from marketing any lottery to U.S. residents or marketing any product or service to U.S. residents in violation of the FTC Act, Telemarketing Sales Rule or Arizona and Washington consumer protection statutes. The court ordered defendants to pay nearly $3.2 million in consumer redress, but the parties ultimately agreed to redress of $500,000, which had been frozen by the B.C. Ministry of Attorney General, to be released to the FTC.

---

[136] *See United States v. Ernest Levy et al.*, [2002] O.J. No. 2298 (Ontario Sup. Ct. Justice – C. Campbell J.) (affirmed by the Court of Appeal - 10 January 2003). In its opinion enforcing the judgment, the Superior Court of Justice explained :

> The trend in Canadian Courts has been in recent years to broaden rather than narrow recognition and enforcement of foreign judgments, particularly those of the U.S. government or its agencies that are restitutionary in nature.
>
> . . .
>
> The principle of disgorgement judgments based on U.S. agency proceedings as been recognised in Canada in several decisions and is not seriously contested by the Defendants on this motion.

- Press Release (Complaint): http://www.ftc.gov/opa/1998/11/win3.htm
- Press Release (Final Judgment): http://www.ftc.gov/opa/2001/02/win2.htm

* * *