

WRITTEN TESTIMONY OF

**LAWRENCE E. MAXWELL
POSTAL INSPECTOR IN CHARGE**

**FRAUD, CHILD EXPLOITATION, AND
ASSET FORFEITURE DIVISION
U.S. POSTAL INSPECTION SERVICE**

**U.S. SENATE PERMANENT SUBCOMMITTEE
ON INVESTIGATIONS**

HEARING ON CROSS-BORDER FRAUD

JUNE 14, 2001

Introduction

The U.S. Postal Inspection Service, the Nation's oldest federal law enforcement agency, greatly appreciates the opportunity to present testimony to the Permanent Subcommittee's Hearing on Cross-Border Fraud. We are grateful for the many past efforts of the subcommittee, under the leadership of Senator Collins and Senator Levin in the area of consumer protection. The Inspection Service was most pleased with the passage of the Deceptive Mail Prevention and Enforcement Act which became effective last year, and with the fine work this subcommittee continues to do on behalf of the American Public.

The Scope of the Problem

The issues surrounding cross-border fraud are not only timely today, but foreshadow what we may expect tomorrow. The marvels of communication technology that improve our lives, also provide the means for crime schemes to cross any national border, quickly and with anonymity. Predatory solicitors are aggressively victimizing American citizens and businesses from outside the protection of our national borders by telephone, through the mail, and over the Internet. They remain faceless to their victims. The predatory techniques utilized by these operators are similar in scope to those the subcommittee uncovered in the hearing held in the 106th Congress on the *Hidden Operators of Deceptive Mailings*. In fact, we have found through investigations of cross-border fraud that quite often the victim pool comes from people who have in the past responded to various deceptive mailings within the United States.

The difficulties in accurately measuring the extent of the cross-border problem are the same encountered when measuring the scope of all frauds. The potential for fraud schemes is infinite. We learned through consumer focus groups during the *Know Fraud* Prevention campaign, that many frauds go unreported. Victims either do not know where to report fraud, or they are embarrassed to make it known that they have fallen victim to a fraud scheme. Law enforcement agencies can report the actual number of fraud investigations, arrests, and convictions they conduct each year. Consumer and government agencies can collect and report the number of complaints they receive. We can profile victims and losses in actual cases

as will be discussed later in this testimony. However, in the final analysis, all the information available to us is only a portion of what is a much larger universe.

In the last year, the Postal Inspection Service has seen a 105% increase in the number of mail fraud complaints received from victims in the U.S. concerning Canadian promotions. Although these complaints represent only 6% of all fraud complaints received by our Mail Fraud Complaint System, the increase is dramatic and telling. A few years ago, AARP reported that telemarketing fraud costs victims over \$40 billion per year. In the November 1997 *Report of the United States and Canada Working Group on Cross-Border Fraud*, it was recognized that total sales from telemarketing in both countries has grown rapidly, reaching more than \$400 billion in U.S. dollars per year. The group concluded that although most telemarketing activities are legitimate, as much as 10% of the total volume of telemarketing is fraudulent. We know the problem is significant and devastating to its victims. We know there are many who have lost their life savings to the relentless pursuit of telemarketers, and we know with relative certainty the problem will increase if we do not now resolve to address it aggressively.

Criminals utilizing the latest communication systems are able to prey on Americans and remain out of reach of our laws. Sadly, the victims are often those who can least afford it. The elderly on fixed incomes, the disadvantaged, or those simply trying to increase their life savings for retirement needs, appear in disproportional numbers as victims. Unfortunately, as technology improves and becomes more readily available, the number of countries where these predators chose to operate from will increase and so will the number of victims.

We have intelligence that indicates, in light of the laws enacted through the work of this subcommittee two years ago with the Deceptive Mail Prevention and Enforcement Act, mailers who have been operating in the shadows within our country have expanded their operations into the international arena. For example, recently we found a deceptive mail operator from the United States was mailing deceptive solicitations out of Canada to the United Kingdom and Australia. The borders of countries are often used as a shield by the operators. If you live in country A, mail out of

country B, and victimize citizens of country C, you effectively shield yourself from regulation during the period of time needed to execute a scheme to defraud.

The Role of the Postal Inspection Service

One of the oldest domestic and international communications systems – the U.S. Mail – continues to play a key role within the modern global economy. Most electronic commerce and telemarketing promotions still must rely on traditional forms of delivery. Our mail system was designed to assure that there is always a reliable, efficient, affordable and secure means for American citizens to communicate and conduct commerce. For over two hundred years, America's first special agents, later named postal inspectors, have had the responsibility for protecting postal employees, the mails, and postal facilities from criminal attack. Equally important, postal inspectors are entrusted to protect consumers and businesses from being victimized by fraudulent schemes or other crimes involving the mails such as identity theft. We also work to rid the mails of drug trafficking and money laundering; mail bombs; and are regarded as a world leader in the fight against one of the most despicable crimes – child pornography.

Today there are approximately 1,990 postal inspectors, 1,400 postal police officers, and 900 professional, technical and support employees. The Inspection Service has the primary responsibility of enforcing roughly two hundred federal statutes designed to protect the postal communications system of our nation.

Recently, a Harris poll revealed that the American Public feels significantly more confident about the security of the mail than the telephone, Internet or other means of communication. The privacy and protection afforded the mail is more certain and tangible. It is the primary mission of the Postal Inspection Service to preserve that confidence.

Fraud and Deceptive Mail Statutes

The Inspection Service is proud to be the primary enforcer of the first consumer protection law ever enacted – the mail fraud statute (18 U.S.C. & 1341). Interestingly, the need for this protection did not become apparent

until the nation began to grow. Fraud promoters began to cross state borders to avoid local laws and take advantage of the absence of federal laws. As swindlers realized the adaptability of the postal system for perpetrating scams the problem grew worse. The advent of railway mail service in the 1830's allowed businesses to expand their customer networks, and because consumers could not otherwise easily obtain these goods, mail order sales skyrocketed. Unfortunately, many customers were duped by misleading advertisements or charges for merchandise they never received.

In response, Congress enacted the mail fraud statute in 1872, to better enable postal inspectors to protect citizens. Today, the mail fraud statute is used to prosecute everything from stock scams to loan scams, from telemarketing frauds to insurance frauds and many others. Illegal telemarketers and other fraud promoters not only rely on the mails to deliver and receive materials to further their scheme, they often use prize promotion solicitations to obtain identifying information. Once they have the telephone number of a potential victim, they follow-up with telemarketing calls.

Current federal judge and former federal prosecutor Jed S. Rackoff wrote in 1980, "To federal prosecutors of white collar crime, the mail fraud statute is our Stradivarius, our Colt .45, our Louisville Slugger, our Cuisinart-and our true love." Even in an electronic world, the mail fraud statute is the weapon of choice in stopping widespread fraud, and it holds a unique place in the proud tradition of the U.S. Postal Inspection Service. During the past fiscal year, 3,257 investigations were initiated regarding possible mail fraud violations. The same year we obtained 1,377 convictions, resulting in prison sentences, fines in excess of \$135 million, court-ordered and voluntary restitution to victims exceeding one billion dollars.

Our criminal enforcement efforts are not limited to federal prosecutions. We also utilize our expertise in conducting investigations of fraud schemes to provide assistance to state and local authorities in cases being pursued in state courts.

The False Representation and Lottery Statute, 39 U.S.C. & 3005, allows the Postal Service to take administrative action to return to consumers all mail

sent in response to a lottery or a scheme that seeks to obtain money or property by mail through false representations. These proceedings will effectively stop the flow of money to the unscrupulous promoter. These statutes, which were strengthened by this subcommittee with the Deceptive Mail Prevention and Enforcement Act of 1999, now have more teeth as a stronger statute with stiffer penalties, and provide more effective tools for law enforcement.

One of the most effective tools is the administrative subpoena authority, which inspectors now utilize. The Inspection Service quickly made use of your work with the issuance of 31 administrative subpoenas, and the filing of 40 complaints that have resulted in 6 Cease and Desist Orders, and 36 False Representation Orders. Even more significantly, our Fraud Complaint System reflects a decrease of 27% in sweepstakes complaints. Since the focus of the subcommittee on deceptive mailings, we find fewer individuals participating in these promotions, indicating that the required disclaimers are being read by recipients. Clearly, the subcommittee's hearings on deceptive mailings have heightened the awareness of the public to the problem.

The Postal Service Law Department initiates administrative proceedings under this statute before an administrative law judge (ALJ). Following a decision by the ALJ, the matter is sent to the Postal Service Judicial Officer for a final agency decision. For an order to be issued under the statute, the Judicial Officer must determine that the promoter is making the representations alleged and that the representations are materially false. Last fiscal year, complaints filed with the Judicial Officer alleging violations of Section 3005 resulted in 36 consent agreements, 44 cease and desist orders and 23 False Representation Orders.

Because the administrative proceedings may be time-consuming and mail scams often are of short duration, two federal statutes (18 U.S.C. & 1345 and 39 U.S.C. & 3007) authorize the U.S. district courts to issue injunctions to prevent consumer losses while the administrative proceedings are pending. Section 1345 permits injunctive orders ranging from stopping the delivery of mail in response to the fraudulent solicitation to the appointment of a receiver to manage a fraudulent company and provide restitution to victims. Section 3007 allows the U.S. district courts to issue temporary

restraining orders and preliminary injunctions ordering the Postal Service not to send or deliver mail sent in response to schemes that are the subjects of pending actions under the false representation and lottery statute.

In cases where a promoter uses a fictitious name or address in connection with a fraudulent scheme in violation of 18 U.S.C. & 1341 or to escape identification, the Postal Service can withhold mail in response to the scheme pending adequate identification and proof of entitlement to the mail. Administrative remedies under these statutes (39 U.S.C. & 3003 and 3004) were used in 151 cases during the past fiscal year, preventing the promoters' receipt of their intended victims' money.

Through the provisions of the Deceptive Mail Prevention and Enforcement Act, postal inspectors utilized our agency's subpoena authority 31 times and have recently received the first money from penalties levied as a result of the law.

To combat illegal foreign lotteries from victimizing American citizens, U.S. Customs Service officials work with the Inspection Service to stop such offerings from entering the country. U.S. Customs agents contact postal inspectors when they find such mail during border searches. The mail is detained and samples are forwarded to the Postal Service Law Department to determine their legality. If mail is considered illegal, the mailer is notified that the material is subject to destruction and may appeal the notice. If the mailer fails to appeal or loses the appeal, the detained mail is destroyed. Over 107,579 pieces were destroyed during Fiscal Year 2000 alone, and approximately one-half million pieces of foreign lottery mail has been destroyed since 1994.

The Cross-Border Issue

As referenced earlier, the con artists in the early days of our nation capitalized on the lack of federal laws by operating across state boundaries. Today's con artists are beginning to employ the same strategy across international boundaries to victimize Americans and avoid our laws. Like a ripple on a pond, the promotion origination points are gradually spreading farther and farther away from the victims. The Inspection Service and other

agencies are beginning to see an increase in international fraud schemes employing online solicitations while relying on traditional methods of delivery. Unfortunately, when a U.S. citizen sends money to Europe or elsewhere for a product and does not receive it, there is little U.S. law enforcement can do. We need to develop strategies and methodologies to combat the growing problem.

The positive results attained by the subcommittee's efforts to deter deceptive mailings in the United States, may have inadvertently made cross-border promotions more prolific. As the subcommittee pointed out in its hearings on the *Hidden Operators of Deceptive Mailings* in the 106th Congress, anonymity is crucial to the success of many of these operators. As we more effectively pursue deceptive marketing techniques in the United States, deceptive operators find safe harbors by operating outside our borders.

The Inspection Service believes that the best strategy is to begin to build and test the solutions close to home. The United States and Canada share the longest unprotected border in the world. We share common English colonial roots that formed the foundation of our legal systems. And, we share a pioneering spirit and love of free enterprise. For those reasons and our common language, our two nations are well-equipped to develop solutions to emerging international economic crime challenges.

Currently, we see the more traditional fraud schemes coming from Canada. They employ a combination of telemarketing techniques and mailings. The reliance on overnight delivery for payment continues. The fraud scheme types we see most frequently from Canada include low interest credit card and credit repair, advance fee loans, security and investment, prize or sweepstakes, failure to provide, general misrepresentations about a product or service, office supply scams, and lotteries.

In one recent advance fee case investigated in Toronto, the promoters initially used Postal Money Orders as the payment method of preference. They later switched to Western Union Money Transfers. Respondents were directed by promoters to use overnight mail to submit money orders payable to the named company at an address later identified as a commercial mail receiving agency (CMRA). The promoter utilized CMRA

addresses in both the United States and Canada. Of course, no loans were ever issued. The average life of an individual telemarketing operation in this case was 60 days, at which time the principals resurfaced using new names, with new telephone numbers and CMRA addresses. The telemarketers utilized sophisticated cellular phones, pagers, and fax machines.

As U.S. law enforcement pursued telemarketers from state to state over the last three decades, certain trends emerged. The operators tended to develop relationships with one another using fulfillment centers familiar to them to furnish products. Promoters typically did not prey upon victims residing in their own state. In a number of instances we see families pass along the "family business" to succeeding generations. Using a telephone the reach of one telemarketer is boundless. Lists of victims are compiled in what the promoters coldly refer to as "mooch lists." The unfortunate victims are often not allowed to suffer one devastating loss, but are contacted again and again in a relentless manner to extract more money from them with false promises of recovering their loss. The practice is referred to as "reloading." And, somewhat cynically, the venues for this activity are known in the illegal telemarketing world as "recovery rooms."

As fraud operators began appearing in Canada more frequently, postal inspectors and other U.S. law enforcement agents began to reach out to their counterparts in the north. Like our own law enforcement officers, Royal Canadian Mounties, provincial and metropolitan police officers all share the same strong dedication "to serve and protect." In most instances, cooperation between Canadian and U.S. law enforcement has been excellent. However, because of the different laws and sovereignties, U.S. and Canadian officers are limited by jurisdiction in what they can do.

Because the telemarketing/boiler room issue was not a problem in Canada and did not focus on Canadians, there were no existing Canadian laws that proved effective in combating the problem for the Americans. Prosecutors relied upon established methods such as requesting assistance through the Mutual Legal Assistance Treaties (MLATs) and traditional extradition procedures. These methods have proven time-consuming, burdensome, and not as effective as we would like. Difficulties are often encountered in attempting to obtain business records and other evidence by U.S. law

enforcement personnel. By the mid-nineties, it was clear to those closest to the problem that a fix was needed.

An Alliance Against Fraud

While meeting in Washington, D.C. in April 1997, President Clinton and Prime Minister Chretien directed officials to prepare a joint study examining ways to counter the growing problem of cross-border telemarketing fraud. In response to the directive the Cross-border Fraud Working Group was formed. The results of the initial meetings of the Working Group were published in the November 1997 Report of The United States – Canada Working Group to the President and Prime Minister. The report cited that total sales from telemarketing in both countries has grown rapidly, reaching more than \$400 billion in U.S. dollars per year. However, illegal telemarketing was recognized by Canadian and American members of the working group as one of the most pervasive and problematic forms of white-collar crime in Canada and the United States.

The group prepared a list of recommendations which included the following points:

- Both countries to identify telemarketing fraud as a serious crime.
- Exploration of the use of remote testimony in criminal proceedings.
- Exploration of enhancements to the use of electronic surveillance in telemarketing cases.
- Examination of the regulation of telephone services and options for denying telephone services to telemarketing offenders.
- Consider needed modifications to the scope of mutual legal assistance treaties (MLATS).
- Clarification of rules governing the use of MLATS.
- Deportation options for offenders.
- Research into developing education and prevention programs.
- Sharing of strategies between the two countries at both the regional and national levels.
- Ongoing bi-national working group to coordinate efforts.
- Encouragement of regional task forces to cooperate to the extent possible.
- Further coordination through the examination of privacy and other laws relevant to cross-border shared access information systems with consideration to expanding access to the maximum extent possible.

The Cross-Border Fraud Task Force continues to meet. It provides a forum to exchange views, share best practices and develop solutions. The next meeting of this group is scheduled for the week of June 17, 2001, in Ottawa, Ontario, Canada. The Inspection Service pledges to continue to play an active role with this group.

I recently provided the subcommittee with the Inspection Service's perspectives on the success of the Task Force in addressing the fourteen recommendations it identified in 1997. The most significant accomplishment is that law enforcement agencies in both countries have identified telemarketing fraud as a serious crime. Collectively they view the cross-border aspects of the crime as a major challenge to overcome and have resolved to cooperate toward solutions. The Postal Inspection Service and other agencies have assigned agents to task forces in Canada, or encouraged others to develop and maintain contacts with the Royal Canadian Mounted Police (RCMP) or local provincial police forces.

Generally, both countries have demonstrated they view telemarketing as a serious crime by increasing penalties for fraud, through the creation of joint task forces, utilization of shared complaint databases such as the Federal Trade Commission's Consumer Sentinel, and/or Canada's PhoneBusters, conducting consumer education and fraud prevention initiatives, and by publicly acknowledging the significance of the problem.

The difficulties with obtaining U.S. victim witness testimony in Canadian court proceedings can be partially addressed through the use of video-conferencing. As stated earlier, often the victims are elderly and travel is difficult for them. Video-conferencing has been used with success in Canadian courts by having victims testify remotely. An Ontario Crown Counsel has discussed video-teleconferencing in a Cross-Border case to be tried in Ontario. And, a request for assistance was referred to the Middle District of Pennsylvania U.S. Attorney's Office for assistance with a video-conference. Federal evidence laws and procedures allow the use of remote testimony in legal proceedings. However, we still face certain logistical and practical considerations that are being worked out on both sides of the border, on a case-by-case basis. However, some judges just do not feel comfortable with videoconferencing of witnesses and insist on physical

appearances. Funding for witness travel outside the country has become difficult within current agency budget design. This issue will need to be addressed in some fashion.

Federal law now permits electronic surveillance in telemarketing fraud cases without a court order when one party in the conversation consents to the surveillance. In the United States, a court order is required when neither party consents. However, the law in Canada requires a court order for any electronic surveillance, unless both parties consent.

Resolving the legal and practical considerations to allow for the disruption of telephone service of known telemarketing boiler rooms is highly important. It is our understanding that the U.S. Department of Justice has submitted a request to Congress for legislation that would provide authorization to seek court orders to block or terminate telephone service to numbers being used for the conduct of telemarketing fraud. Currently, the only method available in the United States is through an injunction under 18 U.S.C. & 1345. Of course, this is not applicable to Canadian locations.

U. S. authorities (primarily DOJ) have encouraged an examination of the MLAT process that could streamline current procedures and minimize delays. We know of instances where requests have lingered for several years causing frustration on both sides of the border, so clearly the process needs to be streamlined. In the U.S. MLAT request training has been added to the law enforcement training curriculums of the appropriate agencies. Communication channels need to be opened between cross-border counsel and agents. The only incidents where we have been successful in a reasonable amount of time were when contact was made directly with the Crown Counsel assigned to the specific case.

Obtaining the actual evidence for court use still requires going through the treaty. This is a reasonable requirement because it is the only opportunity for the defendant or anyone with an interest in the evidence sought to be turned over, to challenge the legality of its having been obtained (e.g., challenging a wiretap).

Canadian legislation has addressed the expediting of extradition requests; however, we are not aware of any similar initiatives in the United States to

address the cross-border extradition problem. Since the cross-border initiatives began, we have seen some cases move slightly faster than in previous years. Of course, there are still several ways defense attorneys can delay, first by challenging treaty requests for whatever evidence is needed, and then by challenging the extradition to the maximum extent.

The Inspection Service also needs to find a means to enforce its administrative subpoenas in Canada. We recently subpoenaed some Canadian businesses and are currently experiencing some problems with compliance from Canadian companies.

Enforcement Initiatives

There are three established and very active cross-border fraud enforcement initiatives between the United States and Canada. The “theaters of operation” are Montreal, Toronto, and Vancouver.

Project Colt (Montreal)

In January of 1998, the Royal Canadian Mounted Police (RCMP) formed Project Colt, as a multi-agency/cross-border task force targeting Montreal-based fraudulent telemarketing. A large percentage of Canadian fraudulent telemarketing occurs in Montreal, Quebec, Canada. The trend is toward aggressive telemarketing of fewer victims but for larger dollar amounts. Project Colt is based at the RCMP office in Montreal. It was initially comprised of experienced investigators from the RCMP, the Surete du Quebec (SQ), and the Montreal Urban Community Police (MUCP). In May of 1999, agents from the U.S. Postal Inspection Service, U.S. Customs Service, and the Federal Bureau of Investigation (FBI) joined Colt to focus on United States victimization.

Last Fall, RCMP management authorized funding for extensive electronic surveillance efforts. They also ordered a commensurate increase to their officers assigned to the effort. Colt investigations have resulted in criminal charges being brought against Canadians in Kansas, California, and Arizona, and the return of 9.6 million dollars to the victims. Their investigative initiatives resulted in searches and arrests in the Montreal area of members of a large organized promotion that has operated for several years. Since January 1998, Project Colt has been responsible for shutting down 14 boiler rooms in the Montreal area, 75 arrests (U.S. and Canada), and obtained restitution for victims in both countries of approximately \$16 million Canadian (\$10.67 million U.S.). Public loss to Montreal area boiler room promotions as reported to Project Colt or otherwise determined from evidence exceeds \$76 million Canadian (\$50,920,000 U.S.).

The benefits of the close working relationships between the two countries' law enforcement agencies and the wealth of intelligence and experience they are acquiring cannot be overemphasized. A recent successful Project Colt case netted extensive media coverage which is another way to educate the public by drawing attention to the matter. On the morning of February 9, 2001, a Canadian subject was arrested by postal inspectors and FBI agents while vacationing at the Grand Floridian Hotel in Disney World, Orlando, Florida. The arrest was made in execution of a warrant obtained on complaint of a postal inspector in the District of Massachusetts. The complaint charged violations of Title 18, U.S. Code, Sections 371

(conspiracy), 1341 (mail fraud), 1342 (using or assuming a fictitious name or address in connection with mail fraud or unlawful business), and 1343 (wire fraud).

This was one of several arrests and searches executed the same day, with all the rest executed by a force of over 100 law enforcement officers in the area of Montreal. The evidence in support of the complaint was principally obtained as a result of an intense three-month investigation in the Montreal area by the Canadian police agencies which were provided to members of Project Colt. The investigation involved extensive electronic surveillance.

The alleged scheme involved a "recovery pitch" to victims of previous prize promotions. Telemarketers, disguised as lawyers, court officers or law enforcement officers, or other government officials, telephoned prospective victims, principally elderly Americans. The promoters told the prospective victims that the callers have come into possession of substantial sums of money which rightfully belong to the prospective victims. In order to claim their money, the victims were told they must send sums of money ranging in amounts from thousands to tens of thousands of dollars to the callers' nominees.

Evidence gained from the electronic surveillance, as set forth in the affidavit in support of the complaint, indicated that from January 9 through 30, 2001, forty-six (46) individuals in the United States sent a total of \$436,278 to various addresses in the Montreal area set up in connection with the original scheme. Additionally, another 208 individuals indicated they were interested in participating and would attempt to arrange to obtain and send to Montreal an amount that would total another \$2,978.039 in the same three-week period.

Another key Colt strategy is the network that has been set-up to intercept victim payments clearing Canadian Customs enroute to the promoters. Overnight delivery companies are notified of the fraud and the payments are withdrawn by the RCMP.

The analysis and case leads stemming from the efforts of Project Colt will continue to assist both countries stem the tide of telemarketing.

The Strategic Partnership (Toronto)

In October 2000, the Postal Inspection Service was pleased to sign a Memorandum of Understanding (MOU) officially joining the Strategic Partnership. In addition to the Inspection Service, the Partnership members include the Toronto Police Service, the Ontario Ministry of Consumer and Business Services, Industry Canada, and the U.S. Federal Trade Commission, Ontario Provincial Police, and PhoneBusters. The Partnership is based in Toronto, Ontario, Canada. The staff is not permanently based in Toronto, but rather affiliated from their respective home bases and coordinate investigative activities centered in Ontario Province.

The predominant fraud emanating from Toronto according to the FTC's Consumer Sentinel involves advance fee telemarketing schemes. In one case, a Toronto based group targeted U.S. victims, taking fees and offering loans, which never materialized. On February 23, 2000, Toronto police executed four search warrants on a boiler room operated by the firm. Nine suspects were arrested and charged with fraud. In coordination with the U.S. Postal Inspection Service, the Canadian charges were subsequently stayed and the suspects will be extradited to the U.S. on charges of mail fraud. The federal grand jury sitting in Harrisburg, Pennsylvania returned an indictment on April 11, 2001. This investigation resulted from information received from the FTC and the Postal Inspection Service regarding victim complaints. Industry Canada provided information from their database and open files, and PhoneBusters provided the initiative with information on the companies and additional victim information.

Since February 2000, over \$550,000 (Canadian) has been seized for victims from Partnership investigative efforts. Moreover, approximately 36 boiler rooms have been completely shut down.

In the first Partnership case that resulted in a criminal indictment, an article appearing in the May 11, 2001 edition of the Toronto Sun was titled "*U.S. posties sign on to help T.O. cops.*" The case involved an advance fee telemarketing promotion that began with published advertisements appearing in the United States that offered loans for individuals with bad credit. Callers responding were told they need to pay an advance fee but never heard from the firm once they paid the fee. The scheme netted \$2

million from victims over a two-year period. Ten Toronto residents were charged as a result of the investigation.

Although it predated the formation of the Strategic Partnership, Operation GEMSCAM was successfully conducted with the contributions of many of the Partnership members. Operation GEMSCAM was the work of an international investigative task force led by the U.S. Postal Inspection Service and the Royal Canadian Mounted Police that spanned an eight-year period. Significant assistance was provided by the Toronto Police Service, PhoneBusters, the Royal Cayman Police and the Federal Trade Commission. As a result of the investigation, the Middle District of Pennsylvania announced 11 indictments and 16 criminal informations charging 125 defendants (97 Canadian Nationals) for fraudulent “liquidation story” telemarketing activity.

The “liquidation story” is used to make additional sales or collect advance fees from vulnerable victims who possess unmarketable investments, i.e., gemstones, “precious” metals and bulletin board stocks. The telemarketers falsely promised the “liquidation” of the investments at a substantial profit upon completion of these purchases or advance fee payments. Confirmed losses to 5,000 United States, Canadian and European victims exceed \$100 million.

To date, over \$4 million has been distributed to victims as restitution. An additional \$3 million in restitution and fines exceeding \$550,000 have been ordered by the United States District Court. Convicted telemarketers have been sentenced to terms of imprisonment ranging from three to fifty-one months.

Additional encouragement for the excellent cooperation shown by the Partnership will be given when it will be presented with the prestigious National Association of Consumer Agency Administrations (NACAA) Consumer Agency Achievement Award at the end of this month.

Vancouver Task Force (Vancouver)

The third initiative in Canada is known as Project Emptor. It is based in Vancouver, B.C., Canada. It is comprised of five members of the RCMP,

an investigator from the Provincial Attorney General's Office of Consumer Protection, and an investigator from Industry Canada. U.S. participants include the Postal Inspection Service, the FBI, and the FTC. There is a preponderance of lottery and bond related investigations. To a lesser extent, intelligence has shown a telemarketing crime problem involving products- everything from pills to television sets.

In August of 1998, the Inspection Service concluded one of the largest cross-border fraud cases to date with the conviction of James Blair Down of Vancouver, B.C., Canada and Barbados. Mr. Down pled guilty in federal court in Seattle for his part in the operation of a fraudulent lottery marketing enterprise. Down sold international lottery products to U.S. residents through illegal interstate transportation of gambling material. Using trade names such as "The Lottery Connection," "Winners," "New Eagle," "International Fortune Bureau" and "Project Rainbow." Down's staff operated from telephone rooms in Vancouver and Kelowna, B.C., and Toronto, Ontario, Canada. They marketed chances, shares and interests in Canadian, Australian, Spanish, Irish and various U.S. lotteries, mostly to senior citizens.

As part of his plea agreement with the government, Down forfeited \$11.7 million, to be paid in restitution to the victims of the scheme. Moreover, an additional \$1 million seized in New Jersey became part of a forfeiture settlement after that portion of Down's promotions was investigated for fraud. During the investigation, Seattle postal inspectors learned that Down's victims averaged 74 years of age, losses ranged from \$10,000 to \$329,000 and the average charge for lottery products was \$50,000. Although initially beset with challenges, the case is viewed today as a success story of how cooperation in cross-border crime investigations can work. Mr. Down was sentenced in the United States but was allowed to serve his prison sentence in Canada.

Conclusion

The Inspection Service has been involved with the cross-border fraud issue for several years. It was a natural evolution as we followed the trail of the fraud promoters. As pointed out earlier, technology has provided new opportunities for those bent on conducting fraud schemes to victimize

greater numbers while remaining relatively hidden. There are several areas we offer the subcommittee to consider as you contemplate what attention may be needed to this issue that is impacting so many American citizens.

The Inspection Service enthusiastically supports the continuation of the existing Cross-Border Forum and its associated working groups. The dialogues, relationships, joint enforcement efforts and improvements stemming from the first years of this group demonstrate its great value. The Inspection Service commends the U.S. Department of Justice for taking the leadership of the U.S. delegation. It was a visionary step.

We commented earlier on the status of the recommendations made by the first cross-border working group. These issues are still relevant. However, several areas require additional sustained attention before real improvement can be realized. Some may require legislation and some simply the continued cooperation of the working groups. They include:

- A funding solution for witness travel and videoconferencing. Perhaps a solution might include authorization to set aside criminal fine money resulting from telemarketing cases to use for this purpose.

- Continued enhancement to the existing MLAT agreement.

- Explore remedies, legal and technological, to disrupt telephone service of known boiler rooms or illegal telemarketing operations.

- Enhance communication channels between cross-border counsel and agents.

- Streamline the process to obtain requested records and testimony.

- Encourage additional regional and functional partnerships. The Consumer Sentinel and PhoneBuster partnership is a great success story.

- Encourage law enforcement agencies and consumer groups to share complaint information.

- Establish joint fraud investigative training initiatives to include Canadian and U.S. law enforcement personnel together. The combined programs will promote a cohesive and unified approach to the problem. Further, it will establish relationships, encourage the sharing of strategies, and instill an understanding of the requirements of both nations' legal systems.

Alternative Remedies

The crime of fraud is substantially different from a crime of violence such as robbery. In a fraud, the consumer makes a conscious decision to participate or not. Time is on their side. A choice is offered and a decision must be made before there can be a victim. The right decision can only be an educated decision. It is the challenge of law enforcement, consumer groups and government leaders to educate consumers not to become victims. Therefore, through fraud prevention programs we can continue to reduce the number of victims. Together, we need to continuously reinforce the prevention message.

Prosecutors and judges share this belief as well. Several years ago a major mail fraud investigation was concluded involving a telemarketing advance fee scheme. Nearly four million dollars was seized for forfeiture. The large number of victims eliminated the practicality of restitution. Therefore, the assistant United States attorney in the case recommended to the Inspection Service that the government should forfeit the money and hold it in a separate Fraud Forfeiture Prevention Fund. The court sanctioned the agreement as did the Department of Justice. By an agreement with the court the money was to be used first and foremost for fraud prevention and consumer education programs. Short of that, it was permissible to use the funds to investigate fraud promotions. Indeed, an innovative approach to preventing future victimization.

During the subcommittee's hearing on Deceptive Mail, the Chief Postal Inspector announced for the first time that the Inspection Service was leading an interagency alliance in the largest consumer protection campaign ever attempted. *Project Know Fraud* was launched in November of 1999 with public service announcements and a national press conference that included the Postmaster General, the Attorney General, and representatives of all the partners- FTC, FBI, SEC, BBB, and AARP. There were approximately 100 other coordinated press events around the nation. The first *Know Fraud* campaign consisted of a postcard with important consumer tips on how individuals can protect themselves and their loved ones from illegal telemarketing solicitations. It included a toll free number to call for more information or to register a complaint, a Web site, and much

more. The card was mailed to every household in the nation- 120 million addresses.

In July, we will be launching a second *Know Fraud* campaign focusing on the fastest growing crime identity theft. The strategy is to continue to evolve the *Know Fraud* concept on an ongoing basis and build on the consumer awareness momentum. One approach is to select areas of the country where there are inordinately large numbers of victims for a certain type of crime, for example, victims of telemarketing fraud from Canadian promoters. A Town Hall Meeting will then be scheduled to address the type of prevalent crime schemes in that area and how individuals can protect themselves or report incidents. The Inspection Service intends to explore Canadian interests in partnering in the *Know Fraud* prevention initiatives. It would provide an excellent forum to share information and educate consumers on both sides of the border to protect themselves.

Local prevention initiatives are oftentimes more effective in addressing the local needs. In the Inspection Service Pittsburgh office just such an initiative was launched. Members of the Senior Action Coalition and the Postal Inspection Service assembled a packet of materials on how seniors can protect themselves from be victimized by fraud schemes tailored just for them. The one brochure contained a compelling photograph of a senior with the caption "He lived through two world wars, fought in one. He helped raise six children and three dogs. He saved a long time for his retirement. Don't let one phone call take it all away." The other information included the Inspection Service brochure on Preventing Mail Fraud and SEC's Cold Calling Alert, and others.

Many other initiatives have been aimed at victims susceptible to this type of scheme. For example reverse boiler rooms are used very effectively throughout the United States. The reverse boiler room works by using "mooch lists" obtained from prosecuted telemarketing operations, and calling the names to warn them of the risks of illegal telemarketing. Often federal, state and local prosecutors participate. In certain instances celebrities or government officials participate to help make it a "media event" that will spread the message more effectively to a wider audience.

One theme was pervasive throughout our consumer protection campaigns- a large percentage of the American public do not know where to report frauds, and there seem to be too many complaint databases. We need to simplify the process for the consumer. Also, one of the recommendations of the working group was to share intelligence. Accordingly, the Postal Inspection Service and the FTC recently signed a memorandum of understanding to share fraud complaint information. This agreement formalizes a partnership that has evolved over the last several years. Both agencies lead Project Know Fraud and share many similar initiatives. Consumer Sentinel also has a partnership with Canada's PhoneBusters.

The FTC has recently expanded its Consumer Sentinel System with an international capability making it more useful to U.S. and Canadian law enforcement and regulatory agencies that investigate telemarketing. However, we recently learned from the cross-border task force that Article 29 of the Canadian Competition Act appears to create significant impediments to information-sharing by Canadian and U.S. authorities. To be successful in combating cross-border frauds we will need to come up with alternatives to address such challenges while waiting for any necessary legislative changes that benefit consumers.

The Inspection Service has a unique position as a member of the International Postal Community to enhance security and develop alternative strategies. For example, the notorious 4-1-9 fraud letter from West Africa has plagued most industrialized countries for the last several years. Little could be done using traditional methods. The Chief Postal Inspector, in his position as President of the Postal Security Action Group of the Universal Postal Union, developed a cooperative strategy whereby the postal administrations of the affected countries worked toward a solution together. The group quickly agreed that the fraud letters bore counterfeit postage, and agreed to allow for their seizure and destruction using existing postal policies and procedures, enhanced through memorandums of understanding (MOUs). Since that time over five million letters have been seized and destroyed. The problem in the mails has been reduced significantly. Unfortunately, now the promoter have moved the scheme onto the Internet.

The Inspection Service is now using that “postal family connection” to develop solutions to the cross-border problem. We have been working closely with Canada Post on finalizing a MOU to allow for combined uses of our civil administrative powers to stop fraudulent mail. For example, ideally we want to stop victim mail from reaching the promoter in Canada. Our authority cannot cause the mail to be stopped in Canada. We are working on a means where Canada Post will utilize their Prohibitory Order authority on addresses we have targeted from the U.S. This strategy has great potential of saving numerous individuals from ever becoming victims in the first place.

Moreover, the Inspection Service has three standing partnerships with industry groups to work together to reduce losses from fraud and theft. The three groups include the Mail Order Task Force, the Rebate Fraud Task Force, and the Credit Card Task Force. Each has its own success story of reducing fraud losses and sharing best practices. For example, the now familiar concept of credit card activation was the result of a postal inspector working with the Credit Card Task Force. Canadian agencies and business have begun to show interest in joining these groups. They have attended several of the meetings. A cross-border make-up would be highly advantageous in attacking the fraud problems of North American and the Inspection Service will encourage this prospect.

The Postal Service just concluded an exhaustive process to enhance its regulations governing the registration and delivery to commercial mail receiving agencies (CMRA's). CMRA addresses frequently appear in fraud investigations. In fact, case examples in this testimony illustrate how cross-border fraud promoters utilize CMRA addresses to carry on their schemes and avoid detection. The Inspection Service intends to inform our Canadian counterparts of the reasoning behind the changes. Ideally, Canada may conclude that similar regulation would be beneficial for CMRA's operating in that country. The primary achievement of the regulatory change was the requirement for the address designation “PMB” for private mailbox, or “#” if preferred by the addressee. This will provide added protection to consumers that the address they are mailing to is a CMRA.

The Postal Inspection Service and its Project Colt partners are presently working on an effort with the cooperation of Western Union to add internal

procedures to help prevent and detect the international transfer of victim monies. They also work closely with UPS and FedEx. Overnight delivery is the principle method of payment used by schemers to circumvent law enforcement efforts to intercept physical payments prior to delivery. The Postal Inspection Service also has a formal agreement with Peace Bridge Brokers which provides Canadian Customs clearance on overnight Purolator mail deliveries. Postal Money Orders, however, remain a victim remittance of choice. Our Money Order Division has worked closely with investigators to detect recent money laundering trends, and curtail the negotiation of domestic money orders in Canada.

Finally, as stated earlier, the Inspection Service views the cross-border issues currently being addressed with Canada, as the precursor to similar crimes originating in other countries around the world. We also see the strong need to include consideration of the Internet in any strategy we develop. Crimes originating online will continue to increase and provide a means to cross any national border.

The Postal Inspection Service commends the members of the subcommittee for focusing attention on this very significant issue. We greatly appreciate being invited to contribute our experiences and recommendations.

