Identity-Related Crime: A Threat Assessment

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

November 2010

Table of Contents

Executive Summary

For more than a decade, identity-related crime – sometimes called "identity theft" or "identity fraud" – has been growing into a crime problem that significantly affects not only North America, but countries around the world.

In 2003, the Cross-Border Crime Forum focused attention on the problem of identity-related crime by directing its Mass-Marketing Fraud Subgroup to prepare a threat assessment.[1] Because identity-related crime continues to expand, the Forum directed the Subgroup in 2008 to prepare an updated threat assessment.

This threat assessment focuses on five aspects of the identity-related crime problem as it affects Canada and the United States: (1) the scope and extent of the problem; (2) the purposes of identity-related crime; (3) the categories of individuals who engage in or are victimized by identity-related crime; (4) the methods and techniques that criminals use to commit identity-related crime; and (5) the responses to the problem. Its purpose is to identify and describe the most problematic features of this crime problem, as well as the approaches being used in both countries to combat it.

Annually, a significant percentage of the U.S and Canadian populations is the victim of some kind of identity-related crime. The continuing vulnerability and insecurity of various types of payment mechanisms and identification documents is one of the persistent problems in combating identity-related crime. Criminals and criminal organizations engage in a wide variety of identity-related crime to commit fraud, unlawfully obtaining goods, services, or benefits from the public or private sector.

Individuals as well as private and public sector players can all play meaningful roles in reducing the risk of, and combating, identity-related crime. It is important for countries to ensure not only that they have effective and useful legal tools to investigate and prosecute the crime, but that their residents are educated about and have effective mechanisms for engaging in self-help or seeking assistance to recover from the crime.

With each passing year, identity theft, and the individuals and organizations behind it, become more complex and capable of rapid adaptation to changing circumstances. Government (especially law enforcement) and private-sector entities in both countries need to follow suit. When losses to individuals, businesses, and government from identity theft – including the collateral harm to reputation and costs of repairing and restoring identities – can be measured in the tens of billions of dollars each year, both the public and private sectors have ample incentive to work together, and to build collaborative relationships with their counterparts in other countries around the world, to combat this problem.

---

[1] *See* BI-NATIONAL WORKING GROUP ON CROSS-BORDER MASS MARKETING FRAUD, REPORT ON IDENTITY THEFT: A REPORT TO THE MINISTER OF PUBLIC SAFETY CANADA AND THE ATTORNEY GENERAL OF THE UNITED STATES (October 2004), *available at* http://www.publicsafety.gc.ca/prg/le/bs/report-eng.aspx.

Introduction

For more than a decade, identity-related crime – sometimes called "identity theft" or "identity fraud" – has been growing into a crime problem that significantly affects not only North America, but countries in multiple regions of the world. In 2003, the Cross-Border Crime Forum focused attention on the problem of identity-related crime by directing its Subgroup on Mass-Marketing Fraud to prepare a threat assessment.[2] Because identity-related crime continues to expand in Canada, the United States, and other countries, the Forum directed the Subgroup in 2008 to prepare an updated threat assessment.

This threat assessment will focus on five aspects of the broad problem of identity-related crime as it affects Canada and the United States: (1) the scope and extent of the problem, including its effects on individuals and corporate and government entities; (2) the purposes of identity-related crime; (3) the categories of individuals who engage in or are victimized by identity-related crime; (4) the methods and techniques that criminals use in committing identity-related crime; and (5) the responses to the problem by the public and private sectors. Its purpose is to identify and describe the most problematic features of this crime problem, as well as the approaches that law enforcement, government, and private entities are using in both countries to combat the problem.

Defining Identity-Related Crime

Throughout history, criminals have often engaged in the unauthorized acquisition and use of another person's identity to obtain some advantage they are not entitled to receive. Adopting the identity of another to commit crime not only conceals the true identity of the criminal, but can mislead law enforcement authorities into believing that the victim of the crime is in fact the criminal.

Beginning in the late 1990s, as credit cards and other forms of remote payment became increasingly popular, and the criminal misuse of those payment mechanisms became increasingly prevalent, government, the public, and the media in the United States increasingly referred to the phenomenon of identity misuse as "identity theft."[3] While the term "identity theft" is now ubiquitous in Canada and the United States,[4] these and other countries have also used the term "identity fraud" to refer to various aspects of the criminal misuse of identity.[5] The two terms,

---

[2] *See* BI-NATIONAL WORKING GROUP ON CROSS-BORDER MASS MARKETING FRAUD, REPORT ON IDENTITY THEFT: A REPORT TO THE MINISTER OF PUBLIC SAFETY CANADA AND THE ATTORNEY GENERAL OF THE UNITED STATES (October 2004), *available at* http://www.publicsafety.gc.ca/prg/le/bs/report-eng.aspx.

[3] *See, e.g.*, Identity Theft and Assumption Deterrence Act of 1998, Pub. L. (October 30, 1998), *codified at* 18 U.S.C. 1028(a)(7).

[4] *See, e.g.*, Department of Justice Canada, Press Release (January 8, 2010) (press release reporting coming into force of Bill S-4), *available at* http://www.justice.gc.ca/eng/news-nouv/nr-cp/2010/doc_32470.html (English) and http://www.justice.gc.ca/fra/nouv-news/cp-nr/2010/doc_32470.html (French); Federal Trade Commission, Identity Theft, *available at* http://www.ftc.gov/bcp/edu/microsites/idtheft/.

[5] *See, e.g.*, Australian Institute of Criminology, Identity fraud, *available at* http://www.aic.gov.au/crime_types/economic/idfraud.aspx; CIFAS, Identity Fraud, *available at*

however, are not synonymous. Both popular and legal definitions of identity theft tend to focus on the misuse of real persons' identities. In recent years, law enforcement authorities have observed a growth in the use of synthetic identities – that is, spurious identifying information that is not related to a real person – to commit various types of fraud. In addition, the term "identity fraud" is sometimes used to refer to any type of fraud that involves the misuse of a real or synthetic identity. And, under Canadian law, effective January 2010, "identity theft" is the unauthorized possession, trafficking or use of personal information and "identity fraud" is the fraudulent use of another person's personal identification to gain advantage, obtain property, disadvantage another person, avoid arrest or defeat or obstruct the course of justice.[6]

To ensure consistency throughout this threat assessment, the term "identity-related crime" will be used to encompass both identity theft and identity fraud, whether defined in legal or practical terms. This usage is consistent with the practice of multinational government bodies with law enforcement interests, such as the G-8 Justice and Home Affairs Ministers[7] and the United Nations Office on Drugs and Crime Core Group of Experts on Identity-Related Crime.[8]

I. The Scope and Extent of Identity-Related Crime

Identity-related crime, as described in greater detail below, can be defined as a cycle with five distinct phases: (1) unauthorized or illegal acquisition of identifying data or items (e.g., cards or documents); (2) transfer of the initially acquired identifying data or documents; (3) manipulation of the data or items (e.g., through alteration, compilation, or forgery/counterfeiting); (4) transfer of the manipulated data or items; and (5) use of the data or items for fraud or concealment of criminal identity.[9]

To date, there have been limited government studies from Canadian and U.S. government entities regarding the scope and extent of identity-related crime in North America. In the United

---

http://www.cifas.org.uk/default.asp?edit_id=566-56; Directgov, Identity fraud, *available at* http://www.direct.gov.uk/en/CrimeJusticeAndTheLaw/Typesofcrime/DG_174616; Royal Canadian Mounted Police, Identity Theft and Identity Fraud, *available at* http://www.rcmp-grc.gc.ca/scams-fraudes/id-theft-vol-eng.htm (English) and http://www.rcmp-grc.gc.ca/scams-fraudes/id-theft-vol-fra.htm (French); U.S. Department of Justice, Identity Theft and Identity Fraud, *available at* http://www.justice.gov/criminal/fraud/websites/idtheft.html.

[6] *See* Bill S-4, An Act to amend the Criminal Code (identity theft and related misconduct *available at* http://www.justice.gc.ca/eng/news-nouv/nr-cp/2010/doc_32471.html (English) and Projet de loi S-4, Loi modifiant le Code criminel (vol d'identité et inconduites connexes) *available at* http://www.justice.gc.ca/fra/nouv-news/cp-nr/2010/doc_32471.html (French).

[7] *See* G8 Justice and Home Affairs Ministerial Meeting – Concluding Declaration (June 13, 2008), *available at* http://g8.gc.ca/about/past-summits/ministerial-meetings-2008/justice-home-affairs/.

[8] *See, e.g.*, United Nations Commission on Crime Prevention and Criminal Justice, Third meeting of the Core Group of Experts on Identity-Related Crime (Vienna, Austria, 20-22 January 2009), *available at* http://www.unodc.org/documents/treaties/organized_crime/ECN152009_CRP12.pdf .

[9] *See* Criminal and Legal Affairs Subgroup, G8 Lyon-Roma Anti-Crime and Terrorism Group, Essential Elements of Criminal Laws to Address Identity-Related Crime (February 2009) (Annex).

States, the Department of Justice's Bureau of Justice Statistics (BJS) has collected nationwide data since 2004 on the prevalence of households affected by identity theft.[10] The Federal Trade Commission also sponsored two national surveys, in 2003 and 2006, collecting data on the prevalence of identity theft among a random sample of U.S. adults age 18 or older.[11] More recently, a survey by a private research firm, Javelin Strategy & Research, using the methodology developed by the Federal Trade Commission, found that in 2009, a total of 11.1 million U.S. adults (representing 4.81 percent of the U.S. population) had become victims of some form of identity fraud, with an aggregate loss (to both individuals and corporate victims) of US $54 billion.[12] Both the number and the percentage of victims were the highest since Javelin began conducting its annual surveys of identity fraud in 2003.[13] A 2008 survey of Canadian consumers by McMaster University found that nearly 1.7 million people (6.5 percent of the population) were the victim of some kind of identity fraud in the preceding year.[14]

Consumer complaints in both countries provide further indications of the scope and extent of the problem. In 2009, the U.S. Federal Trade Commission (FTC) received 278,078 consumer complaints about identity theft – by far the largest single category (21 percent) of consumer fraud complaints it received. These totals were less than the number of 2008 complaints (314,484), but more than the number of 2007 complaints (259,314).[15] The FTC data do not include data on self-reported victim losses. The Canadian Anti-Fraud Centre (CAFC), formerly PhoneBusters, – a joint forces operation consisting of the Royal Canadian Mounted Police (RCMP), the Competition Bureau Canada, and the Ontario Provincial Police – reported that in 2009, it had received 11,979 identity theft complaints, in which there were 11,909 reported victims. These totals were less than the number of 2008 complaints (12,232) and victims (11,463), but more than the number of 2007 complaints (10,637) and victims (10,328).[16] The

---

[10] *See* Bureau of Justice Statistics, Identity Theft Reported by Households, 2007- Statistical Tables (June 30, 2010), *available at* http://bjs.ojp.usdoj.gov/content/pub/pdf/itrh07st.pdf. In 2008, BJS also collected national data on the prevalence, cost, and victim response to identity theft from a nationally representative sample of individuals age 16 or older. The results from that study are expected to be available by the end of 2010.

[11] *See* Federal Trade Commission, 2006 Identity Theft Survey Report (Nov, 2007), *available at* http://www.ftc.gov/os/2007/11/SynovateFinalReportIDTheft2006.pdf.

[12] See JAVELIN STRATEGY & RESEARCH, 2010 IDENTITY FRAUD SURVEY REPORT at 7 (February 2010).

[13] *See id.* at 8.

[14] *See* Susan Sproule and Norm Archer, Measuring Identity Theft in Canada: 2008 Consumer Survey - Working Paper #23, *available at* http://www.merc-mcmaster.ca/working-papers/measuring-identity-theft-in-canada-2008-consumer-survey/.

[15] See FEDERAL TRADE COMM'N, CONSUMER SENTINEL DATA BOOK FOR JANUARY – DECEMBER 2009 at 4-5 (February 2010), *available at* http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2009.pdf.

[16] *See* CRIMINAL INTELLIGENCE ANALYTICAL UNIT, CANADIAN ANTI-FRAUD CENTRE, ANNUAL STATISTICAL REPORT 2009: MASS MARKETING FRAUD & ID THEFT ACTIVITIES at 23 (2010), *available at* http://www.phonebusters.com/english/documents/AnnualStatisticalReport2009_001.pdf (English) and http://www.phonebusters.com/francais/documents/AnnualStatisticalReport2009fr_000.pdf (French).

CAFC also reported that identity theft victims reported nearly CA $10.9 million in losses – greater than in 2008 (more than CA $9.6 million) or 2007 (nearly CA $6.5 million).[17]

Some data suggest that direct losses to consumers from identity fraud – such as long-term losses from bank or financial accounts -- may be declining. The Javelin report stated that mean consumer costs from identity fraud "dropped sharply in 2009 to $373 from $498 in 2008, a 25% decline."[18] The report inferred from these data "that the [financial] industry is absorbing more fraud loss to limit the impact on consumers. For example, Javelin's 2009 scorecard showed that for the first time, 100% of the top 25 financial institutions surveyed offer zero liability fraud guarantees for debit cards."[19]

Direct financial losses, however, often are less problematic for victims than the indirect costs stemming from the identity thieves' misuse of the victims' personal data to obtain goods, services, or government or private benefits. In the United States, the Javelin report stated that since 2007, new account fraud (i.e., fraud stemming from the misuse of victim's data to obtain new payment cards or establish new bank accounts or loans) had increased by 38 percent, accounting for a total growth of US $6 billion in losses, and "is the main driver of the overall increase in total dollar fraud."[20] While new account fraud does not result in losses from the victims' own legitimate accounts, the misuse of the victims' personal data can result in decisions by other lenders or businesses that adversely affect the victims, such as denials of credit or tarnishing of reputations.

In addition, victims of identity-related crime may have to bear more than *de minimis* costs stemming from efforts to clear their good names and credit ratings. In Canada, the 2008 McMaster survey reported that Canadian victims of identity fraud spent more than CA $150 million of their own money and spent 20 million hours to resolve the fraud in the preceding year.[21] In the United States, the 2010 Javelin survey found that in 2009 the mean consumer cost to U.S. victims was US $373 and the mean time to resolve the identify fraud was 21 hours per victim.[22]

---

[17] *See id.*

[18] *See* JAVELIN STRATEGY & RESEARCH, *supra* note 12, at 8.

[19] *Id.*

[20] *Id.* at 10.

[21] *See* Canwest News Service, *Identity theft plagues Canadians as online shopping grows*, Canada.com, September 18, 2008, *available at* http://www.canada.com/story.html?id=b7f81191-421a-48f5-abc3-8b156c8f6fc2.

[22] *See* JAVELIN STRATEGY & RESEARCH, *supra* note 12, at 7.

II. Purposes of Identity-Related Crime

A. Fraud

The predominant reason that criminals engage in identity-related crime is to commit fraud: that is, to make use of others' true identities or synthetic identities for financial gain through the unlawful obtaining of goods, services, or benefits from the public or private sectors. Both Canadian and U.S. complaint data demonstrate the wide range of fraud to which identity-related crime contributes.

In Canada, the CAFC reported that the benefits that identity thieves obtained with personal information in 2009 included banking and financial benefits (i.e., bank accounts; bank account takeovers; cash; checks; credit cards; false applications for accounts, credit cards, lines of credit, and loans; lines of credit; loans; and mortgages) government and private-sector benefits (i.e., driver's licenses; health cards; insurance; passports; and rerouted mail), jobs, merchandise, and telephone service (i.e., cellphones; false applications for cellphones; and telephone numbers).[23] Similarly, in the United States, Javelin reported that identity thieves used victims' information to commit credit card fraud (76% percent), phone or utilities fraud (11 percent), bank fraud (14 percent), Internet service or payment accounts fraud (15 percent), loan fraud (7 percent), and other types of fraud, including government benefits, medical services, and employment-related fraud (4%) [24]

B. Concealment of Identity

But identity-related crime also provides criminals with significant non-financial benefits. Some acquire or use stolen or fraudulently obtained identification documents and cards to facilitate travel during or after the criminal acts. Others do so with the object of increasing the difficulty of effective investigation by law enforcement in multiple jurisdictions.

- In 2008, a Canadian citizen attempted to enter the United States from Canada, but was found during the inspection process to possess eight counterfeit credit cards, which contained account numbers that had been stolen in Canada, and a counterfeit Quebec driver's license. After the individual admitted that he intended to use the counterfeit cards in the United States, he pleaded guilty in U.S. federal court to identity theft and was sentenced.[25]

---

[23] *See* CRIMINAL INTELLIGENCE ANALYTICAL UNIT, CANADIAN ANTI-FRAUD CENTRE, *supra* note 16, at 24.

[24] *See* JAVELIN STRATEGY & RESEARCH, *supra* note 12, at 12, 29, 35 and 39. These percentages include both new and existing accounts.

[25] *See* U.S. Attorney's Office, Northern District of New York, Press Release (January 4, 2010), *available at* http://www.justice.gov/usao/nyn/NewsReleases/Attachments/144-129-1731359488.pdf.

- In 2009, an individual used the name and rank of an officer in the Canadian Snowbirds 431 Squadron demonstration team in conducting an online scheme in which the individual purported to be selling a car from the United Kingdom.[26]

- In 2010, three Bulgarian nationals, two of them residing in Toronto, were indicted in U.S. federal court on charges of using counterfeit ATM cards, bank fraud, and aggravated identity theft in connection with a skimming scheme in which they are alleged to have compromised numerous ATMs throughout eastern Massachusetts and stolen more than $120,000.[27]

Still others consciously use the identities of others because they can abuse financial accounts or obtain government benefits in their victims' names and misdirect law enforcement or court officials into looking for the wrong persons.

- In 2002, a Florida woman was arrested and detained on an outstanding warrant related to a car theft. In fact, another woman, who had been in Florida penitentiaries four times, reportedly had stolen the car in question while using the victim's identity, and when arrested gave the victim's name. She continued to use the victim's name when she was charged with auto theft, pleaded no contest, and was placed on three years' probation. Even the woman's probation officer knew her under the victim's name. On the day of the victim's arrest, however, the thief reportedly was serving an eight-year sentence in a Florida prison for a series of crimes. The victim, who resembled the thief in certain respects, was released within a day after her mistaken arrest.[28]
- In 2006, a man in Newfoundland reportedly was charged with stealing from a Wal-Mart store in Carbonear, Newfoundland, though he had never visited either the store or the town. Charges were dismissed after the man told police and the media that his wallet had been stolen months earlier, during a break-in at the restaurant where he worked. The arrest, however, reportedly caused his name to be placed on a "no-fly" list.[29]

---

[26] *See* Stephen Pate, *Canadian Snowbirds victim of identity theft in car scam*, NJN Network, June 26, 2009, *available at* http://njnnetwork.com/2009/06/exclusive-canadian-snowbirds-victim-of-identity-theft-in-car-scam/.

[27] *See* U.S. Attorney's Office, District of Massachusetts, Press Release (January 24, 2010), *available at* http://www.justice.gov/usao/ma/Press%20Office%20-%20Press%20Release%20Files/Feb2010/IndictmentPR.html.

[28] *See* Rene Stutzman, *Innocent woman sues after identity theft leads to jailing, strip search*, Palm Beach Post, September 7, 2010, *available at* http://www.palmbeachpost.com/news/crime/innocent-woman-sues-after-identity-theft-leads-to-900829.html.

[29] *See St. John's identity theft victim faces new frustrations*, CBC, January 25, 2010, *available at* http://www.cbc.ca/canada/newfoundland-labrador/story/2010/01/25/nl-theft-norman-012510.html.

C. Support of Criminal Organizations

1. Organized crime

Although not every instance of identity-related crime is attributable to criminal organizations – many identity thefts, in fact, are committed by lone individuals or small, loosely-knit groups[30] – there is no question that criminal organizations play a substantial role in identity theft and fraud. In Canada, the Criminal Intelligence Service Canada (CISC) recently stated in its 2010 Report on Organized Crime:

> Organized crime groups are known to produce, supply or use false identities. . . . Organized crime uses three main methods: modification of some aspect of their own identity; creation of a wholly fictitious identity; or theft of someone else's identity, either living or dead. These false identities assist organized criminals to avoid detection by law enforcement, particularly when traveling and to protect their assets from confiscation. Individuals also use false identification to carry out or enable criminal activity where evidence of an identity is a key requirement, such as fraud, financial crimes, or human smuggling. Other forms of misrepresentation may also be used, such as false information on company or vehicle identity, consignments, business accounts and transactions.[31]

In the United States, a U.S. Department of Justice official, in 2009 Congressional testimony, cited the involvement of criminal groups in the United States and abroad as one of the principal factors in the recent explosion of identity-related crime.[32] Criminal groups in the United States have not only been active in identity theft and payment-card fraud, but have expanded into health-care fraud, where they can misuse doctors' identities for large-scale fraudulent billing.[33]

---

[30] For example, in 2005, a brother and a sister, one a Nigerian national, organized and carried out an elaborate scheme that used personal information fraudulently obtained from ChoicePoint Service and other companies to commit identity theft against thousands of victims. The sister posed as a real estate agent so that she could fraudulently open accounts with several public records database firms, then obtain personal information on thousands of individuals. She then sold the personal information to her brother and other individuals around the country for between $40 and $65. The brother, working with his sister, opened "mail drops" in Beverly Hills and Encino, where he would redirect mail from victims' credit card companies. Once he obtained victims' credit card numbers, he fraudulently made purchases and obtained cash advances. *See* U.S. Attorney's Office, Central District of California, Press Release (March 7, 2005), *available at* http://www.justice.gov/usao/cac/pressroom/pr2005/042.html.

[31] CRIMINAL INTELLIGENCE SERVICE CANADA, REPORT ON ORGANIZED CRIME 2010, *available at* http://www.cisc.gc.ca/annual_reports/annual_report_2010/fundamentals1_2010_e.html.

[32] *See* Statement of Jason M. Weinstein, Deputy Assistant Attorney General, Criminal Division, U.S. Dep't of Justice, Before the Subcommittee on Oversight and Information Policy, Census and National Archives of the House of Representatives Committee on Oversight and Government Reform (June 17, 2009), *available at* http://www.justice.gov/criminal/pr/speeches-testimony/documents/06-17-2009weinstein.pdf.

[33] *See* Allan Chernoff and Sheila Steffen, *Organized crime's new target: Medicare*, CNN, October 24, 2009, *available at* http://www.cnn.com/2009/CRIME/10/22/medicare.organized.crime/.

In addition, a 2010 multinational threat assessment on mass-marketing fraud reported that "Canadian and United States law enforcement investigations have also identified virtual criminal enterprises that consist of individuals around the world who only communicate via online forums yet engage in organized fraud schemes and identity theft."[34]

2. Terrorism

For law enforcement authorities in both countries, the use of identity-related crime to support terrorist activities remains a substantial concern.[35] In 2007, for example, three United Kingdom residents were sentenced to prison for terms ranging from 6 ½ to 10 years, after pleading guilty to charges involving their use of "phishing"[36] web sites, computer viruses, and stolen credit card accounts to establish a network of communication forums and Web sites, which "hosted everything from tutorials on computer hacking and bomb-making to videos of beheadings and suicide bombing attacks in Iraq."[37] More recently, in 2009, a California woman who ran a vehicle registration company was charged by federal and local prosecutors for her alleged operation of an extensive fraud ring involving several Department of Motor Vehicles employees whom she regularly paid to produce licenses and other documents. According to one police official, the names of at least some of her alleged clients have surfaced in ongoing investigations into national security issues.[38]

---

[34] INTERNATIONAL MASS-MARKETING FRAUD WORKING GROUP, MASS-MARKETING FRAUD: A THREAT ASSESSMENT at 16 (June 2010), *available at* http://www.stopfraud.gov/news/immfta.pdf.

[35] *See, e.g.*, Royal Canadian Mounted Police, *Identity Theft and Identity Fraud*, *available at* http://www.rcmp-grc.gc.ca/scams-fraudes/id-theft-vol-eng.htm.

[36] According to the Anti-Phishing Working Group, an internal coalition of corporate entities and government agencies dedicated to combating online-related fraud and identity theft, "phishing"

> is a criminal mechanism employing both social engineering and technical subterfuge to steal consumers' personal identity data and financial account credentials. Social‐engineering schemes use spoofed e-mails purporting to be from legitimate businesses and agencies to lead consumers to counterfeit websites designed to trick recipients into divulging financial data such as usernames and passwords. Technical – subterfuge schemes plant crimeware onto PCs to steal credentials directly, often using systems to intercept consumers' online account user names and passwords – and to corrupt local navigational infrastructures to misdirect consumers to counterfeit websites (or authentic websites through phisher – controlled proxies used to monitor and intercept consumers' keystrokes).

ANTI-PHISHING WORKING GROUP, PHISHING ACTIVITY TRENDS REPORT: 4TH QUARTER 2009 at 2 (2010), *available at* http://www.antiphishing.com/reports/apwg_report_Q4_2009.pdf.

[37] Brian Krebs, *Terrorism's Hook Into Your Inbox*, Washington Post, July 5, 2007, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2007/07/05/AR2007070501153.html. *See* Nicola Woolcock, *Three students jailed for inciting terrorism on 'Holy War' websites*, The Times, July 6, 2007, *available at* http://www.timesonline.co.uk/tol/news/uk/crime/article2034011.ece.

III. Perpetrators and Victims of Identity-Related Crime

There is no single type of perpetrator or victim of identity-related crime. Perpetrators range from first-time offenders to career criminals. Victims, for their part, range from infants (whose U.S. Social Security Numbers or Canadian Social Insurance Numbers are misused by their parents or others) to the elderly. Unlike some types of fraud that may target a particular age group or ethnic group, identity-related crime causes harm to all demographic segments of society. The Javelin 2010 Fraud Survey Report found that in 2009, 3.2 percent of persons aged 18 to 24 became identity-theft victims, as did 5.9 percent of persons aged 25 to 34, 5.3 percent of persons 35 to 44, 6.2 percent of persons 45 to 54, 4.3 percent of persons 55 to 64, and 2.9 percent of persons aged 65 or older.[39] CAFC data for 2009 showed: persons 19 and under accounted for just 2 percent of all identity-theft victims, persons in their twenties accounted for 17 percent, persons in their thirties accounted for 22 percent, persons in their forties accounted for 25 percent, 50s were 18 percent, 60s were 10 percent, and persons 70 and older accounted for about 7 percent of all identity theft victims.[40]

Moreover, businesses as well as individuals may be targeted for identity-related crime. To heighten the legitimacy of their fraud schemes, some criminals freely use the names and account numbers of businesses. For example, a substantial number of advance-fee fraud schemes operating in multiple regions of the world provide their victims with counterfeit checks, to persuade the victims that they are receiving the winnings of a prize contest or lottery, or the payment for online sales, that they were promised.[41] Although the checks are counterfeit, the names, addresses, and bank account numbers that they bear frequently belong to legitimate companies. If these checks bore the names and account numbers of real individuals, there is no doubt that their use of personal data could be prosecutable as identity theft under current law in multiple jurisdictions.

IV. Methods and Techniques of Identity-Related Crime

The G8 Roma-Lyon Group Report on Essential Elements of Law to Address Identity-Related Crime defined identity-related crime as a cycle with five distinct phases: (1) unauthorized or illegal acquisition of identifying items (e.g., cards or documents) or data; (2) transfer of the initially acquired identifying data or documents; (3) manipulation of the items or data (e.g., through alteration, compilation, or forgery/counterfeiting); (4) transfer of the manipulated items or data; and (5) use of the items or data for fraud or concealment of criminal identity.[42] This section of the Threat Assessment will briefly discuss each of those phases.

---

[38] *See* Joel Rubin, *Counter-terrorism investigators find alleged identity theft ring*, Los Angeles Times, July 26, 2009, *available at* http://articles.latimes.com/2009/jul/26/local/me-fraud26.

[39] *See* JAVELIN STRATEGY & RESEARCH, *supra* note 12, at 73.

[40] Information courtesy of the Canadian Anti-Fraud Centre.

[41] *See* INTERNATIONAL MASS-MARKETING FRAUD WORKING GROUP, *supra* note 34, at 4, 10.

A. Acquisition of Personal Information

All identity-related crime must begin, at some time, with the acquisition of valuable personal information by criminals. Their methods of doing so vary widely, depending on the technological skill and sophistication of the criminal and the manner in which those data are stored and accessible. Some criminals seek to target repositories of large amounts of personal data for unauthorized access, or to use methods enabling them to build their own data repositories for resale of those data or for criminal use. To do so, they may use technological skills to hack into databases or use malicious computer code to gain access, "social engineering" skills to trick members of the public into voluntarily disclosing their own data or to develop relationships with and compromise corporate or government insiders with access to large data repositories, or a combination of both. Other criminals, lacking those skills, may content themselves with low-skill methods of acquiring personal data, ranging from break-ins to pickpocketing to mail theft to persuading people to disclose data voluntarily. Here are some recent examples:

- In 2010, a federal grand jury in St. Louis indicted a defendant on charges of multiple fraud charges involving the theft of stolen credit and debit cards from local vehicles, changing the PIN numbers and account addresses, then obtaining more than $45,000 from the accounts of seven individuals through ATM cash advances and withdrawals and purchases of merchandise and gift cards. According to the indictment, the defendant and confederates allegedly went to parking areas used for major public events and watched for drivers who left wallets or purses, then broke into the vehicles once the drivers left the area and stole credit cards, debit cards and identification cards with social security numbers, while leaving the wallets and purses intact.[43]

- In 2010, someone reportedly stole from a British Columbia hospital a laptop that contained data on more than 600 patients, including names, birth dates and personal health card numbers. The data reportedly were neither encrypted nor password-protected.[44]

- In 2010, a federal court in Albany, New York sentenced a defendant to 70 months imprisonment for his involvement in an identity theft ring, after he had pleaded guilty to identification document fraud, wire fraud, and aggravated identity theft. According to

---

[42] *See* Criminal and Legal Affairs Subgroup, G8 Lyon-Roma Anti-Crime and Terrorism Group, *supra* note 9, at Annex.

[43] *See* U.S. Attorney's Office, Eastern District of Missouri, Press Release (August 19, 2010), *available at* http://www.justice.gov/usao/moe/press_releases/archived_press_releases/2010_press_releases/august/parker_jerod.html.

[44] *See 600 B.C. patients' data in stolen laptop*, CBC News, September 2, 2010, *available at* http://www.cbc.ca/health/story/2010/09/02/bc-stolen-laptop-patient-data.html.

court documents, the defendant admitted that he was a team leader in a so-called "flip, bite, and write" identity theft scheme in which ring members targeted elderly women shopping in grocery stores. In brief, teams led by the defendant traveled to locations where retail stores, usually ones that sold groceries, were located in close proximity to stores where electronics could be purchased, such as Best Buy, Circuit City, or Sears. Typically, a member of the defendant's team distracted the elderly female victim in the store ("the flip"), while the defendant stole the woman's credit cards ("the bite"). The defendant then went to his vehicle nearby and, using a laptop and ID printer, made a false identification document in the victim's name with a picture of one of the ring members traveling with him. The false identification documents that he created included state driver's licenses and United States Armed Forces identification cards. Using the stolen credit cards and fake identification, the defendant and his team members then purchased expensive electronics, miscellaneous merchandise, and gift cards, signing the victim's name to the credit card receipts ("the write").

- In 2010, a federal grand jury in Atlanta indicted two individuals on charges of stealing the identities of more than 80 individuals in the Atlanta metropolitan area and opening credit card accounts, loans, and bank accounts in the names of the stolen identities. According to the indictment, one of the defendants obtained a job as a mail carrier, under the name of another woman whose identity the defendant had stolen before the defendant entered the United States in 2004. More than 80 victims on the defendant's mail route reported that their identities were stolen and used to open financial accounts.[45]

- In 2010, a defendant already serving a prison sentence on other charges reportedly was sentenced in the Ontario Court of Justice to additional prison time, after he pleaded guilty to fraud charges relating to a scheme to use the identifying information of more than 1,400 other inmates to apply for federal income and Goods and Services Tax returns and claim about $1.8 million in refunds over several years. The defendant reportedly persuaded other inmates that he would prepare and submit returns on their behalf so that they could receive tax refunds. In fact, the defendant changed the inmates' mailing addresses so that he and confederates could submit the returns under the inmates' names but collect the refund checks for themselves.[46]

B. Transfer of Initially Acquired Items or Data

In many cases, the data, physical cards, or documents that identity thieves have acquired are not ready for immediate use. Depending on how the identity thief wants to profit from the unauthorized acquisition, he may need to gather the data or physical items so that they can be

---

[45] *See* U.S. Attorney's Office, Northern District of Georgia, Press Release (May 12, 2010), *available at* http://www.justice.gov/usao/gan/press/2010/05-12-10.pdf.

[46] *See* Tony Van Alphen, *Inmate earned thousands filing fake tax forms from prison*, Toronto Star, September 16, 2010, *available at* http://www.thestar.com/business/article/861943--inmate-earned-thousands-filing-fake-tax-forms-from-prison?bn=1.

physically transferred elsewhere, or extract the relevant data from them so that they can be transmitted electronically. For example, in numerous phishing schemes, criminals download code onto targeted computers that not only captures the keystrokes of greatest value (e.g., login names and passwords for online bank accounts) but causes those data to be emailed to an online address of the criminals' choosing.

- In 2006, a defendant pleaded guilty in federal court in Richmond, Virginia, to computer fraud and aggravated identity theft. The defendant's statement in support of his plea included a description of his installation of keylogger software on a university's computers, e-mailing the information obtained with the keylogger software to several e-mail accounts that he controlled, and use of the information obtained with the keylogger software to access several password-protected university computer systems and the e-mail accounts of fellow university students and staff.[47]

C. Manipulation of Transferred Items or Data

In order to make use of the acquired data or items, criminals may need first to manipulate the data or items they possess in one of three ways: (1) altering them (e.g., altering identifying or address data on bank or credit-card accounts, or altering data on the face of checks or identification documents); (2) compiling them (e.g., collating data for resale through so-called "carding" websites,[48] or collecting stolen payment cards for distribution to confederates along with fake identification cards); or (3) forging or counterfeiting them (e.g., forging email addresses for online solicitation of prospective fraud victims, or manufacturing payment cards encoded with magnetic-stripe data belong to legitimate payment cards).

- Over a three week period this summer in three separate incidents police in one British Columbia community recovered flash drives and stolen point of sale terminals containing compromised payment card data for more than 20,000 cards. In one related arrest the suspects had most of the equipment needed to counterfeit cards, in another arrest the suspect was in possession of 34 cards which were not in his name.[49]

---

[47] *See* U.S. Attorney's Office, Eastern District of Virginia, Press Release (September 27, 2006), *available at* http://www.justice.gov/usao/vae/Pressreleases/09-SeptemberPDFArchive/06/20060927owusu_georgenr.pdf.

[48] *See, e.g.*, Statement of Rita M. Glavin, Acting Assistant Attorney General, Criminal Division, U.S. Department of Justice, Before the Subcommittee on Emerging Threats, Cybersecurity, and Science & Technology of the House of Representatives Committee on Homeland Security at 4 (March 31, 2009), *available at* http://www.justice.gov/criminal/cybercrime/glavinStatement.pdf.

[49] *See* Kelly Sinoski, *Massive credit card fraud ring suspected in Abbotsford*, August 11, 2010, *available at* http://www.cbc.ca/consumer/story/2010/03/11/consumer-credit-card-scams.html.

D. Transfer of Manipulated Items or Data

In some cases, criminals who intend to carry out fraud schemes that require wide geographic dispersion of their planned fraudulent transactions (e.g., use of counterfeit payments cards at ATMs in multiple cities) will need to transfer the manipulated cards or documents to confederates or the manipulated data to vendors such as "carding" sites.

- In a 2009 Canadian incident, payment card information from approximately 5000 cards was skimmed at a British Columbia restaurant over a period of more than five months. The card information was used to counterfeit cards which were then fraudulently and systematically used by a criminal organization in both Montreal, Quebec and Toronto, Ontario in a coordinated attack which lasted only one half hour, yet resulted in fraud losses of more than $250,000.[50]

E. Use of Items or Data

Finally, of course, criminals will make use of the data or physical items to commit fraud (as described earlier) or other crimes against individuals, businesses, or government agencies, or to engage in other activities, such as travel, for which they need to conceal their true criminal identities.

- In 2010, a California man who claimed to be affiliated with an underground gang of hackers was arrested on federal extortion charges. The criminal complaint in the case alleges that he hacked into dozens of computers, obtained personal data about people using the computers, and then demanded sexually explicit videos from female victims in exchange for keeping their personal information private.[51]

- In 2010, 6 individuals from Edmonton were charged with operating a forgery ring that had stolen hundreds of identities. A search of a downtown Edmonton home yielded counterfeiting equipment and hundreds of forged documents and cards. One suspect was in the process of forging cards which would have enabled the unauthorized acquisition of firearms and ammunition. Investigators also seized a variety of credit cards, grocery store club cards, rewards cards and employee swipe cards which could have been used as corroborating identification for fraudulent loans.[52]

---

[50] This example of a credit card "bust-out" fraud was provided by the RCMP Commercial Crime Branch.

[51] *See* U.S. Attorney's Office, Central District of California, Press Release (June 22, 2100), *available at* http://www.justice.gov/usao/cac/presssroom/pr2010/097.html.

[52] *See* Conal Piers, *Six charged in Edmonton identity theft ring*, Edmonton Journal, June 24, 2010, *available at* http://www.edmontonjournal.com/business/charged+Edmonton+identity+theft+ring/3192865/story.html.

V. Efforts to Combat Identity-Related Crime

A. Reporting Identity-Related Crime

In Canada, there are two principal mechanisms at the federal level to encourage reporting about identity-related crime. First, the Canadian Anti-Fraud Centre, established in 1993, is the central agency in Canada that collects information and criminal intelligence on mass marketing fraud (telemarketing), advance fee fraud letters (e.g., West African), Internet fraud and identity-related crime, that have Canadian content, from North American consumers and/or victims. The CAFC, which is jointly managed by the RCMP, the Ontario Provincial Police, and the Competition Bureau of Canada, does not conduct investigations, but provides valuable assistance to law enforcement agencies all over the world. The CAFC plays a key role in educating the public about specific fraudulent schemes and in collecting and disseminating victim information, statistics and documentation, to provide investigative assistance to all law enforcement agencies. The data collected and analyzed at the CAFC provide a valuable tool in evaluating the effects of various types of fraud on the public, and help to prevent future similar crimes from taking place.[53]

Second, the RCMP maintains an online fraud reporting mechanism that was previously available through the Reporting Economic Crime OnLine (RECOL) web site. RECOL allowed members of the public to file fraud reports online which would then be reviewed by analysts, uploaded to one of the RCMP's national intelligence databases and also disseminated to the applicable enforcement agency for its attention and consideration. In an effort to create efficiencies and eliminate redundancies the functions of the RECOL website were merged with the functions of the CAFC's web site. Today members of the public need only go to one web site, www.antifraudcentre.ca, to get access to information about fraud and identity crime statistics or awareness and education tools, and to discover the various methods available for reporting fraud and identity crime, including an on-line option.[54]

In the United States, there are several mechanisms at the federal level to encourage or require reports about suspected instances of identity-related crime. First, the Federal Trade Commission, pursuant to section 5 of the Identity Theft and Assumption Deterrence Act of 1998,[55] is authorized to maintain the Identity Theft Data Clearinghouse, a database of complaints to which members of the public may contribute by telephone or online. Complaints are also contributed by the Identity Theft Assistance Center and local law enforcement, and information from various States' Attorneys General databases and the Internet Crime Complaint Center will be added in the future. During the two-year period from 2008 to 2009, the FTC received 592,562 identity

---

[53] *See* Royal Canadian Mounted Police, *Canadian Anti-Fraud Centre's: About Us*, *available at* http://www.antifraudcentre.ca/english/aboutus.html , *voir* Gendarmerie Royal du Canada *Au sujet de Centre Anti-Fraud du Canada, disponible à* www.centreantifraude.ca/french/aboutus.html.

[54] *See* http://www.antifraudcentre.ca (English) and http://www.centreantifraude.ca (French).

[55] Pub. L. 105-318, 112 Stat. 3007 (Oct. 30, 1998), *available at* http://www.ftc.gov/os/statutes/itada/itadact.htm.

theft complaints. The FTC's Identity Theft Data Clearinghouse is available free of charge to US and Canadian civil and criminal law enforcement through its secure online database, the Consumer Sentinel Network, accessible 24 hours a day. Second, the FBI and the National White Collar Crime Center (NW3C) jointly operate the Internet Crime Complaint Center (IC3). IC3 provides an online portal for members of the public to report all types of online crime, including identity-related crime.[56] Third, under federal banking regulations, federally insured or chartered financial institutions are required to file Suspicious Activity Reports with the federal government when they encounter possibly criminal activities affecting their institutions, including identity-related crime. In addition, a private entity, the Identity Theft Assistance Center, seeks to assist identity theft victims and will share certain data about the victims' situations with law enforcement.[57]

B. National, Binational, and Multinational Coordination

1. National

Within each country, there are certain established mechanisms to facilitate interagency coordination on identity-related crime issues. In Canada, the National Mass Marketing Fraud Strategy Working Group (the Working Group) has operated since September 2005. A national strategy was developed in January of 2006 by the Working Group to be revisited after three years. The 2006 strategy was based on 4 pillars, those being Vigorous Enforcement, Raised Awareness, Judicial Impact and Improved National Data. In January of 2009 the Working Group revisited the original strategy and made modifications based on previous achievements, existing gaps and the current state of fraud and identity crime. As a result, a new, revised, and more focused strategy based on 3 key pillars was developed. The strategy now is now centered and on a main Intelligence pillar. The Working Group determined that intelligence was essential to the success of the strategy and that intelligence would drive the direction of the other 2 pillars, those being Enforcement and Prosecution along with Prevention through Education and Awareness. In Canada, identity-related crimes are an increasing challenge with detrimental consequences. Cooperation between law enforcement, the public and private sector partners and Canadian citizens is vital to effectively combat and prevent identity crimes. As a result, a shared framework for a national strategy, modeled on Canadian National Mass Marketing Fraud Strategy has been formulated by key stakeholder agencies. These various agencies provide distinct insights into the challenges posed by identity crimes. Reflecting stakeholder input and the strategy on which it is modeled, the National Identity Crime Strategy has three components or "pillars": 1) Criminal Intelligence and Analysis, 2) Prevention through Education and Awareness, and 3) Effective Enforcement, Disruption and Prosecution. For each pillar, areas of concern have been outlined along with some goals and key initiatives/activities to realize these objectives. One goal, for example, is to enhance effective gathering and sharing of identity crime information among law enforcement, private and public sector partners. The overarching vision and purpose of the National Identity Crime Strategy is to improve Canada's ability to prevent,

---

[56] *See* Internet Crime Complaint Center, http://ic3.gov.

[57] *See* Identity Theft Assistance Center, *available at* http://www.identitytheftassistance.org/.

detect and deter identity crimes. The strategy itself is the start in laying the foundation for change and betterment.

In the United States, since October 2008 there has been an Identity Theft Enforcement Interagency Working Group. This working group, which the Fraud Section of the Department of Justice's Criminal Division chairs, meets monthly in Washington, D.C. to bring together all of the principal federal law enforcement, regulatory, and executive departments and agencies for regular information exchanges on key trends and developments in identity-related crime. Each month, the Working Group has presentations, either in person or by videoconference, from Assistant U.S. Attorneys in various districts across the United States. These presentations, in which field-office representatives of federal investigative agencies sometimes participate, provide the Working Group with regular updates on key identity-related crime trends across the country. In addition, the Working Group discusses developments relating to law enforcement responses to identity-related crime, identity-related crime victim issues, legal and legislative concerns, and training or other activities in which agency members may wish to participate.

In addition, in 2008 the United States Attorney's Office for the Eastern District of Pennsylvania, in cooperation with the U.S. Postal Inspection Service and others, announced the launching of the National Identity Crime Law Enforcement (NICLE) Network. In NICLE's day-to-day operations, data concerning stolen or criminally used identity information are uploaded from collecting agencies to NICLE through the MAGLOCLEN computer network. Those data will include national law enforcement-generated information, submitted by local, state, and federal agencies, and banking information through an industry clearinghouse, the Identity Theft Assistance Center. The data are available to local, state, and federal law enforcement over a secure Internet connection through the Regional Information Sharing System Network (RISS), which is available nationwide to member agencies. NICLE provides a central repository of identity crime-related information, allowing agencies to learn immediately whether a particular piece of identification (driver's license, credit card, address, social security number, etc.) has been reported stolen or used elsewhere in the course of a crime. It also names investigators associated with particular investigations, so that departments and agencies can coordinate across jurisdictional lines when working on crimes involving the same or connected identities or credit card numbers.[58]

In Canada in 2007, the Inter-jurisdictional Identity Management and Authentication Task Force published its *Final Report: A Pan-Canadian Strategy for Identity Management and Authentication, July 2007.* [59] The report "provides a strategy, recommendations and action plan for implementing a pan-Canadian Identity Management and Authentication (IdM&A) Framework that will facilitate client centred, cross-jurisdictional, multi-channel service delivery

---

[58] *See* U.S. Attorney's Office, Eastern District of Pennsylvania, Press Release (July 10, 2008), *available at* http://www.justice.gov/usao/pae/News/Pr/2008/jul/niclerelease.pdf.

[59] *See* Inter-jurisdictional Identity Management and Authentication Task Force's Final Report: A Pan-Canadian Strategy for Identity Management and Authentication, July 2007, http://www.cio.gov.bc.ca/local/cio/idim/documents/idma_final_report.pdf.

for citizens and businesses." The strategy's value to government is that it provides a framework for cross-jurisdictional collaboration and cooperation with respect to the use of common identification elements and authentication. In addition to a decreased risk that services will be compromised, the value to citizens can be described as multi-faceted. There will be improved security of personal identity and identification documents as well as increased efficiency in processing and authenticating identification. As an example of common identification elements and authentication, for birth certificates, most Canadian provinces now use the same basic hard-to-counterfeit, polymer-based certificates with common graphic and security features.

2. Binational

To date, at the strategic level, the sole mechanism for periodic information-sharing on identity-related crime issues has been the Cross-Border Crime Forum (CBCF) Subgroup on Cross-Border Fraud. The Subgroup's initial focus at the outset of the CBCF in 1998 was cross-border telemarketing fraud, but its work has required it to expand its focus to a variety of identity theft projects, including its 2003 Threat Assessment on Identity Theft and special public advisories on various trends in identity theft.

At the tactical level, key Canadian and U.S. law enforcement partners, including the FBI, RCMP, Competition Bureau Canada, Federal Trade Commission, U.S. Postal Inspection Service and state/provincial/ and municipal law enforcement occasionally share intelligence and collaborate on specific identity theft related investigations. Opportunities for such cross-border cooperation have tended to be identified when criminal activity involving identity theft and mass marketing fraud overlap.

3. Multinational

At multilateral levels, there have been occasional efforts to address identity theft as a topic of mutual concern, though these efforts have not been consistently pursued. First, the European Union (EU) and the European Commission have maintained an active interest in identity theft, as evidenced by the EU's first conference on Identity Theft, held in Tomar, Portugal in 2007. Second, the United Nations Office on Drugs and Crime (UNODC) has been actively exploring the development of best practices and materials on identity theft, using a Core Group of Experts on Identity-Related Crime that it established to provide UNODC with expertise on identity theft from multiple countries and disciplines. Third, the G8 Lyon/Roma Working Group issued a report in 2009 that discussed issues relating to criminalization of identity theft and provided guidance to other countries on how they should evaluate their criminal codes and determine whether revisions would be in order to address all aspects of identity theft.

C. Prevention and Mitigation

1. Restricting access to data and physical items

As the President's Identity Theft Task Force noted in 2007, one key aspect of preventing and mitigating the harms of identity theft is to keep valuable personal data out of the hands of

criminals, through decreasing the unnecessary use of key identifiers such as Social Security numbers, improving data security measures in both the public and private sectors, and educating agencies and private entities about how to protect their data.[60] In addition, under the REAL ID Act of 2005, the Department of Homeland Security has promulgated a final rule to establish minimum standards for state-issued driver's licenses and identification cards. These regulations set standards for states to meet the requirements of the REAL ID Act, including (1) information and security features that must be incorporated into each card; (2) proof of identity and lawful status of an applicant; (3) verification of the source documents provided by an applicant; and (4) security standards for the offices that issue licenses and identification cards.[61]

In Canada, the direction provided by the Inter-jurisdictional Identity Management and Authentication Task Force has seen standardized birth certificates. The Task Force's work may drive standardization of document security features and authentication in such a way that the future will see common platforms for other key Canadian identity documents such as driver's licenses and health cards.

2. Public education (e.g., advisories and guides)

In Canada, the primary providers of public education on identity-related crime have been the Fraud Prevention Forum and it members, including the Canadian Banker's Association, Bank of Canada and major banks / financial institutions, payment card issuers, credit bureaus, Better Business Bureaus and law enforcement bodies. The following examples illustrate the range of public education being delivered:

- The Fraud Prevention Forum, chaired by Competition Bureau Canada, each March leads a "Fraud Prevention Month" awareness initiative. The Forum's nationwide initiative uses the full range of communications media and involves more than one hundred member organizations and police services. Preventing identity-related crime has been a Fraud Prevention Forum focus in recent years.
- The Bank of Canada and partners developed and distributed more than 150,000 educational DVDs to Canadian businesses. The "Check to Protect" kit's educational videos included one specifically targeting identity theft. The video is also available for on-line viewing.[62]

---

[60] See PRESIDENT'S IDENTITY THEFT TASK FORCE, COMBATING IDENTITY THEFT: A STRATEGIC PLAN at 22-30 (April 23, 2007), *available at* http://www.idtheft.gov/reports/StrategicPlan.pdf.

[61] *See* Dep't of Homeland Security, *REAL ID Final Rule*, *available at* http://www.dhs.gov/files/laws/gc_1172765386179.shtm.

[62] *See* Fighting Fraud on the Front Lines: A Retailer's Guide, *available at* http://www.bankofcanada.ca/en/video_corp/dbo/dvd_fraud.html, *Voir* Échec à la fraude : à vous de jouer! *disponible* à http://www.banqueducanada.ca/fr/video_corp/dbo/dvd_fraude-f.html.

- The RCMP distributes a comprehensive, downloadable *Personal Information and Scams Protection – a Canadian Practical Guide*.[63]

In the United States, the FTC has played a leading role in identity theft education and prevention, in part through its development and nationwide distribution of materials on identity theft and its maintenance of a comprehensive website with information on how to identify and respond to identity theft. Other federal agencies, including federal banking agencies and the Social Security Administration, also have routinely posted information on their websites to warn members of the public about specific kinds of identity theft.

The Department of Justice also contributes to identity theft education and prevention efforts. The Department's Office for Victims of Crime (OVC) and Office of Juvenile Justice and Delinquency Prevention (OJJDP) have co-sponsored Web forums to share information and best practices on topics focusing on identity theft, including child identity theft. In addition, OVC is leading the Department's efforts to respond to the needs of child identity theft victims by bringing together identity theft experts to explore this emerging issue. The focus of this effort is to identify ways to further protect and respond to the needs of children whose personal identifying information is compromised, thus jeopardizing their credit, job prospects, and civil liberties in the future and to identify the need for further research in this area of victimization.

3. Law enforcement training

Although public education on identity theft is an important component of government's response to the problem, law enforcement also has recognized that law enforcement agencies need specific training on various aspects of identity theft, including the detection of fraudulent identification documents and data and the use of appropriate investigative techniques and methods. In the United States, the Department of Justice not only sponsors annual seminars for federal prosecutors on identity theft at its National Advocacy Center, but also cosponsors periodic one-day training seminars for state and local law enforcement agencies throughout the United States. The National White Collar Crime Center (NW3C) also provides a number of identity theft courses for law enforcement.

In Canada, since 2002, the RCMP has offered its members on-line training on payment card fraud. Since 2006, the on-line course has been available to other Canadian police. The RCMP's Counterfeit Currency Investigators' Course has included a payment card skimming and counterfeiting component for the more than 15 years.

The RCMP's Commercial Crime Investigator's course has also included an identity theft component since 2004. In July 2010, a new on-line course *Counterfeit Travel and Identity Documents* was released for Canadian law enforcement. Developed by the RCMP, this course is made available on-line to the wider policing community through the Canadian Police Knowledge

---

[63] *See* Personal Information and Scams Protection – A Canadian Practical Guide, *available at* http://www.rcmp-grc.gc.ca/scams-fraudes/canad-practical-pratique-guide-eng.htm, *Voir* Protection des renseignements personnels et protection contre l'escroquerie - Guide pratique canadien *disponible à* http://www.rcmp-grc.gc.ca/scams-fraudes/canad-practical-pratique-guide-fra.htm.

Network.[64] Additionally, over the past 5 years several regional conferences have been held on identity-related crimes.

4. Victim assistance (e.g., legal and practical advice)

At present, assistance to identity theft victims is still a service that is not uniformly offered or available to victims. While the FTC offers extensive materials to assist victims with self-help approaches, it cannot offer full-blown legal guidance and assistance to victims who may need extended support to repair the damage to their names and credit. The FTC has published an online *Guidebook for Assisting the Victims of Identity Theft* (Guidebook) for legal aid, legal services, and pro bono attorneys, and victim assistance counselors. The Guidebook provides instructions and sample forms and letters for victim advocates to provide brief direct assistance to identity theft victims who can take basic self-help measures on their own, as well as detailed legal explanations, copies of statutes and regulations, and sample letters for advocates to intervene on behalf of those who cannot resolve their problems through self-help measures.[65] Some regional private-sector organizations, such as the Identity Theft Resource Center in San Diego, do offer more extensive counseling and guidance for victims. Certain age groups – the very young and the elderly – may require more intensive assistance and intervention in some cases.

The situation in Canada is not much different than in the United States. There are some on-line victims' assistance guides, made available by financial institutions, banks, credit bureaus and law enforcement, designed to assist identity-related crime victims to help themselves. Canada currently has no organization like the Identity Theft Resource Center; however there is a private sector project team which has undertaken to create a not-for-profit organization which will operate as The Canadian Identity Theft Support Centre. The project team is currently working with partners including the U.S. Identity Theft Resource Center and key Canadian stakeholders. The official launch of the centre is set for 2011.[66]

D. Enforcement

1. Task forces and working groups

Both countries have adopted the task force approach, already used successfully in both countries to combat mass-marketing fraud, to share law enforcement resources in investigating and prosecuting identity theft. In the United States, there are now dozens of multiagency task forces or working groups that concentrate, in whole or in part, on identity theft. Though identity-related crime is often multi-jurisdictional in nature, in Canada, such crimes are Criminal Code offences

---

[64] *See* New Releases: Coach Officer Training and Counterfeit Travel and Identity Documents - July 9, 2010, *available at* http://www.cpkn.ca/news_e.html#3 *Voir* Nouvellement disponible : Coach Officer Training et Documents de voyage et d'identité contrefaits - 9 juillet 2010, *disponsible à* http://www.cpkn.ca/news_f.html

[65] *Available at* www.idtheft.gov/probono.

[66] Canadian Identity Theft Support Centre, Executive Overview, July 2010.

and fall under provincial jurisdiction to enforce. That is to say, they generally fall to the responsibility of provincial or municipal police. Consequently, in Canada, identity-related crimes are the responsibility of local police service commercial crime/fraud units. In some cases local police services have created separate identity theft units and/or counterfeit payment card units.

Recognizing that identity-related crime, counterfeit payment cards, and currency counterfeiting are closely related, the RCMP approach has generally been to use Commercial Crime Section resources or to attach investigative resources to the existing Integrated Counterfeit Enforcement Teams which are located in Canada's three major urban centres.

E. Legislative Initiatives

1. Canada

On January 8, Bill S-4 came into force. This legislation, according to a Department of Justice Canada statement:

> creates three new "core" *Criminal Code* offences targeting the early stages of identity-related crime, all subject to 5-year maximum prison sentences:
>
> - **Obtaining and possessing identity information** with the intent to use the information deceptively, dishonestly, or fraudulently in the commission of a crime;
> - **Trafficking in identity information**, an offence that targets those who transfer or sell information to another person with knowledge of, or recklessness as to, the possible criminal use of the information; and,
> - **Unlawfully possessing or trafficking in government-issued identity documents** that contain information of another person.
>
> A new power also permits the courts to order, as part of a sentence, that an offender be required to pay restitution to a victim of identity theft or identity fraud for costs associated with their efforts to rehabilitate their identity (e.g., the cost of replacement cards, documents and correcting their credit history). This provision complements existing provisions which permit restitution to be ordered for actual economic or other property losses.[67]

In Canada, proposed legislation, Bill C-29, *An Act to amend the Personal Information Protection and Electronic Documents Act (Safeguarding Canadians' Personal Information Act)*, was introduced in Parliament in early 2010. This legislation would amend Canada's Personal Information and Electronic Documents Protection Act (PIPEDA) by incorporating notification provisions for any "material breach." Organizations governed by the Act would be required to

[67] *See* Department of Justice Canada, Press Release, TOUGHER LAWS TARGETING IDENTITY THEFT COME INTO FORCE (January 8, 2010), *available at* http://www.justice.gc.ca/eng/news-nouv/nr-cp/2010/doc_32470.html.

notify the Privacy Commissioner when there has been a material breach of the security safeguards protecting the personal information controlled by them. They would also be required to notify individuals whose personal information was compromised if "the breach creates a real risk of significant harm to the individual." Significant harm would include financial loss, identity theft and negative effects on credit records. The organizations would also, without the individual's consent, be required to notify any government institution that could reduce the risk of harm or mitigate the harm from the breach.[68]

2. United States

Since 2007, the United States has made a variety of changes in federal criminal law that improve its ability to prosecute identity theft. These changes, which stemmed from recommendations in the 2007 President's Identity Theft Task Force Strategic Plan,[69] were embodied in the Identity Theft Enforcement and Restitution Act,[70] which became law on September 26, 2008. The principal provisions of ITERA include clarification and expansion of jurisdiction for various cybercrime offenses, a directive to the United States Sentencing Commission regarding identity-theft sentences, and authority for federal courts to include in sentences a requirement that a defendant convicted under the general identity theft offenses[71] pay "equal to the value of the time reasonably spent by the victim in an attempt to remediate the intended or actual harm incurred by the victim from the offense."[72]

Within the past 18 months, at least two federal court decisions have affected the application of the federal aggravated identity theft offense, 18 U.S.C. § 1028A. In 2009, the United States Supreme Court held, in *Flores-Figueroa v. United States*,[73] that in prosecuting a defendant under the aggravated identity theft offense, the government must prove that the defendant knew that the "means of identification" (e.g., name, Social Security number, or credit-card number) that the defendant unlawfully transferred, possessed, or used, in fact belonged to "another [real] person."[74] More recently, in *United States v. Magassouba*,[75] the United States Court of Appeals

---

[68] *See* Legislative Summary of Bill C-29: An Act to amend the Personal Information Protection and Electronic Documents Act *available at* http://www2.parl.gc.ca/Content/LOP/LegislativeSummaries/40/3/c29-e.pdf , *Voir* Résumé législatif du projet de loi C-29 : Loi modifiant la Loi sur la protection des renseignements personnels et les documents électroniques *disponible à* http://www2.parl.gc.ca/Content/LOP/LegislativeSummaries/40/3/c29-f.pdf.

[69] *See* PRESIDENT'S IDENTITY THEFT TASK FORCE, *supra* note 60.

[70] *See* Pub. L. 110-326, Title II, §§ 201-209 (September 26, 2008), *available at* http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=110_cong_public_laws&docid=f:publ326.110.pdf.

[71] 18 U.S.C. §§ 1028(a)(7) and 1028A(a).

[72] Pub. L. 110-326, Title II, § 202(3) (September 26, 2008), *codified at* 18 U.S.C. § 3663(b)(6).

[73] 129 S. Ct. 1886 (2009).

[74] *Id*. at 1888.

[75] No. 09-3035-cr, slip op. (2d Cir., decided August 31, 2010).

for the Second Circuit held that in a prosecution under section 1028A, where venue is appropriate for the felony offense that serves as a predicate for the aggravated identity-theft charge (e.g., mail fraud or wire fraud), "so too is venue appropriate for a prosecution of the separate crime of knowingly transferring, possessing, or using a means of identification of another person 'during and in relation to' that offense," even when there is no evidence that the defendant "transferred, possessed, or used another person's means of identification within that district."[76] This decision, in a case of first impression, is important because it provides the necessary authority appropriately to charge identity thieves whose identity-theft and associated criminal conduct takes place in more than one jurisdiction.

VI. Conclusion - The Way Forward: Challenges and Recommendations

A. Improving Document and Data Integrity and Security

One of the persistent problems in combating identity theft, for both the public and private sectors, is the continuing vulnerability and insecurity of various types of payment mechanisms and identification documents. That vulnerability is attributable in part to the nature of the mechanisms and documents themselves, and in part to the vast number of sources from which those mechanisms and documents are issued. In the United States, according to the National Association of Public Health Statistics and Information Systems (NAPHSIS), there are approximately 6,400 state and local jurisdictions that issue vital records such as birth and death certificates. In addition, many of those records typically lack even a standardized format from state to state, let alone security features that would make it difficult for criminals to acquire or misuse them.

Individuals, of course, can play a meaningful role in reducing risks of identity theft. Simple techniques to safeguard personal data, ranging from shredding of unneeded financial records to using Internet security software and other online tools, are tasks that individuals can and should routinely use. But the growing number of instances in which criminals compromise large amounts of valuable personal data, either through insider compromise or external attacks such as hacking and phishing, provide strong evidence that individuals alone cannot be expected to bear the primary burden of stemming the tide of identity theft. Governments at all levels and multiple business sectors – including banking and financial services, information technology, and payments – must recognize that they need to play substantial and complementary roles to accomplish that task.

B. Improving Detection of Fraudulent Identification Documents and Data

Given the continuing problem with insecurity of identification documents and data repositories, it is incumbent on government and the private sector in both countries to seek out or develop mechanisms to detect fraudulent or forged identification documents and payment cards more effectively. Even when identification documents and payment cards lack robust security

---

[76] *Id.* at 2.

measures, new technologies can provide valuable assistance in validating such documents and cards in the short term.

In the United States, recent developments have provided strong indications of the value of facial-recognition technology in combating identity theft associated with driver's licenses. In August 2010, New York Governor David A. Paterson announced the initial results of the state's Department of Motor Vehicles' (DMV's) use of facial recognition technology to identity fraud cases. The DMV's facial recognition software

> essentially converts DMV's digital, facial photographs into mathematical algorithms. The software presents trained staff with photo images that have been identified as having similar algorithms. This review includes new photos taken each day at the DMV, as well as about 15 million photos already in DMV's database. Identity documents associated with a new photo are not produced until any photo identified as a potential match is reviewed by trained staff. The DMV strives to issue each applicant only one identity document and seeking a second identity document is a crime since it requires the submission of a false instrument.[77]

This technology has been instrumental in identifying more than 1,000 cases of possible fraud and making more than 100 felony arrests. Arrests included an Egyptian citizen holding four New York driver's licenses under separate names, one of which was on the federal government's "no-fly" list; a former hit man who sought to establish a second identity after his release from prison; and an individual wanted for a 1990's-era bank robbery in Nassau County, New York. Others charged had license suspensions or a large number of tickets and accidents under multiple identities.[78] The U.S. Department of Transportation's Federal Motor Carrier Safety Administration has made grants to support such efforts by DMVs.

C. Improving Reporting Mechanisms

As described earlier, both Canada and the United States have national reporting centers to receive, review, and make use of complaints from the public about identity theft. While there are already efforts to share information, within the constraints of national law, across borders, authorities in both countries should explore additional avenues by which these reporting centers and other public and private sector mechanisms can timely share relevant information on key identity theft trends and on specific identity theft complaints.

D. Improving Coordination of Intelligence-Sharing, Law Enforcement Cooperation, Public Education Initiative

---

[77] Office of the Governor, New York State, Press Release (August 10, 2010), *available at* http://www.ny.gov/governor/press/081010Dmv.html.

[78] *Id.*

Both countries also should look for opportunities to improve their coordination of identity theft-related investigations and intelligence and expand cooperation between law enforcement agencies, at the subnational, national, and transnational levels:

- At the subnational level, police and law enforcement agencies have often recognized the value of establishing working relationships and information-exchange mechanisms, such as multiagency task forces and working groups, to combat various types of fraud and identity theft. Those types of relationships and mechanisms should be encouraged and, where possible, expanded to provide greater opportunities for timely sharing of tactical and strategic information involving identity theft.

- At the national level, investigative agencies typically have substantial interest in the problem of identity theft, but no single agency is legislatively empowered to take the lead in conducting investigations where the criminal conduct may occur across multiple state or provincial borders. In these circumstances, coordination and information-sharing between national-level agencies need to be strengthened and enhanced, so that all agencies with relevant jurisdiction and expertise may be able to function as efficiently as possible. In the United States, the FTC's Consumer Sentinel's Identity Theft Data Clearinghouse, and the National Identity Crime Law Enforcement (NICLE) Network are providing law enforcement agencies at all levels in multiple states with real-time access to significant identity-theft data that can provide important leads for investigation and opportunities for multiagency coordination.[79]

- Finally, at the transnational level, because identity theft has become increasingly globalized, police, investigative, and prosecutive agencies in multiple countries need to establish mechanisms to ensure timely sharing of strategic and tactical information on identity-theft trends and operations across national borders. Although there can be significant differences in legal regimes regarding privacy protection, law enforcement needs to improve its capacity to track and take action against identity theft transnationally and certain mechanisms can be established to operate in a manner consistent with those legal regimes. Since September 2009, for example, law enforcement agencies in Canada, the United Kingdom, and the United States have been discussing the establishment of an International Identity Crime Working Group. Such a Working Group can provide agencies in those countries, and perhaps in other countries as well, with a regular forum for information exchange, discussion, and identification of specific opportunities for bi- or multinational cooperation to combat identity theft.

Furthermore, law enforcement in both countries will need to explore and develop opportunities for educating all relevant segments of the public -- including not only the general public, but the

---

[79] *See* Audit Division, Office of Inspector General, U.S. Department of Justice, The Department of Justice's Efforts to Combat Identity Theft, Audit Report 10-21 at 14 (March 2010), *available at* http://www.justice.gov/oig/reports/plus/a1021.pdf. As of August 2009, NICLE "contained 6.5 million records and was used by approximately 190 police departments, 26 state agencies in 5 states, and 12 federal agencies." *Id.*

media, the business community, and all branches of government – about the problems that identity theft causes and the measures that individuals and entities can take to counteract the problem. While certain agencies in both countries have played a continuing role in public education and prevention initiatives directed at identity theft, there is as yet no consistent coordination between agencies to ensure consistency and coherence in the preventive and educational messaging that should be directed at individuals, businesses, and government agencies.

E. Continuing Review and Improvement of Legislative Frameworks

Both countries should remain attentive to their legal regimes and look for circumstances which may warrant further revision. For example, in 2007, the President's Identity Theft Task Force recommended that Congress amend the federal identity-theft offenses to ensure that identity thieves who misappropriate information belonging to corporations and organizations can be prosecuted.[80] Although Congress did not include this recommendation in its enactment of the Identity Theft Enforcement and Recovery Act in 2008, criminals continue to misuse corporate names, account numbers, and other data to carry out a wide range of identity theft and fraud that affect both individuals and corporations.

Both Canada and the United States should also encourage other countries to review their respective legislative frameworks to see whether changes are appropriate to ensure that all aspects of identity theft, from initial acquisition of others' personal data to ultimate use, are subject to appropriate criminal sanctions. While many countries have general offenses such as fraud or false pretenses that may apply to the frauds stemming from identity theft, they do not always have appropriate measures to address the initial phases of identity-related crime, as Canada now has in Bill S-4. The 2009 G8 Report on Essential Elements of Law to Address Identity-Related Crime, [81] in which Canadian and U.S. representatives played key roles to develop the concepts and draft the text for adoption by the G8 heads of delegations last year, provides sound guidance for other countries to use in reviewing their criminal codes.

F. Improving Awareness and Availability of Victim Assistance Tools and Remedies

To combat identity theft effectively, it is important for countries to ensure not only that they have effective and useful legal tools to investigate and prosecute the crime, but that their residents who are victimized by identity theft have effective mechanisms for engaging in self-help or seeking assistance as necessary to recover from the crime. This latter requirement is by no means easy to implement, as identity theft can strike victims anywhere they live or work, regardless of their income level or type of employment, and can affect different aspects of the

---

[80] See PRESIDENT'S IDENTITY THEFT TASK FORCE, *supra* note 60, at 67.

[81] Criminal and Legal Affairs Subgroup, G8 Lyon-Roma Anti-Crime and Terrorism Group, *supra* note 9.

components of their identities (e.g., bank accounts, credit cards, and Social Security or social insurance number). Nonetheless, both countries must take the necessary steps.

One concrete step would be to ensure that governments and private-sector agencies provide appropriate guidance and advice to identity-theft victims on how to access information and restore their lives. In the United States, the Federal Trade Commission (FTC) makes available, in both hard-copy and online versions, comprehensive guidance for identity-theft victims. Other agencies, such as state attorneys general, provide similar guidance for victims in their respective states. In Canada, as already indicated, victim assistance information is available from several organizations, for example, in 2010 the RCMP made an on-line Victim Assistance Guide for victims of Identity Fraud available on its web site.[82]

Another concrete step would be to foster greater capability within the legal profession to render competent legal advice to identity-theft victims. Often, victims may be uncertain about their legal rights as victims and the appropriate processes for correcting private-sector and government records. Many people, however, lack the funds to hire a lawyer who represent their interests and can guide them through the business and government processes necessary to restore their identities. In 2007, the President's Identity Theft Task Force recommended that the American Bar Association, with assistance from the Department of Justice, "develop a pro bono referral program focusing on assisting identity theft victims with recovery."[83] In 2008, the American Bar Association adopted a resolution that supported the establishment of pro bono, lawyer referral, and other programs to provide such service to identity theft victims. As part of the effort to implement that program, the Federal Trade Commission, in consultation with the Department of Justice, recently issued a pro bono guide for assisting identity theft victims[84] for use by bar associations through the United States.

* * *

With each passing year, identity theft, and the individuals and organizations behind it, become more complex and capable of rapid adaptation to changing circumstances. Government (especially law enforcement) and private-sector entities in both countries need to follow suit. When losses to individuals, businesses, and government from identity theft – including the collateral harms to reputation and costs of repairing and restoring identities – can be measured in the tens of billions of dollars each year, both the public and private sectors have ample incentive to work together, and to build collaborative relationships with their counterparts in other countries around the world, to combat this problem.

---

[82] *See* Identity Theft and Identity Fraud Victim Assistance Guide, *available at* http://www.rcmp-grc.gc.ca/scams-fraudes/victims-guide-victimes-eng.htm, *Voir* Guide pour les victimes de fraude ou vol d'identité *disponible à* http://www.rcmp-grc.gc.ca/scams-fraudes/victims-guide-victimes-fra.htm.

[83] PRESIDENT'S IDENTITY THEFT TASK FORCE, *supra* note 60, at 49.

[84] *See* Federal Trade Comm'n, Guidebook for Assisting Identity Theft Victims (2010), *available at* http://www.idtheft.gov/probono/docs/i.%20Table%20of%20Contents.pdf.