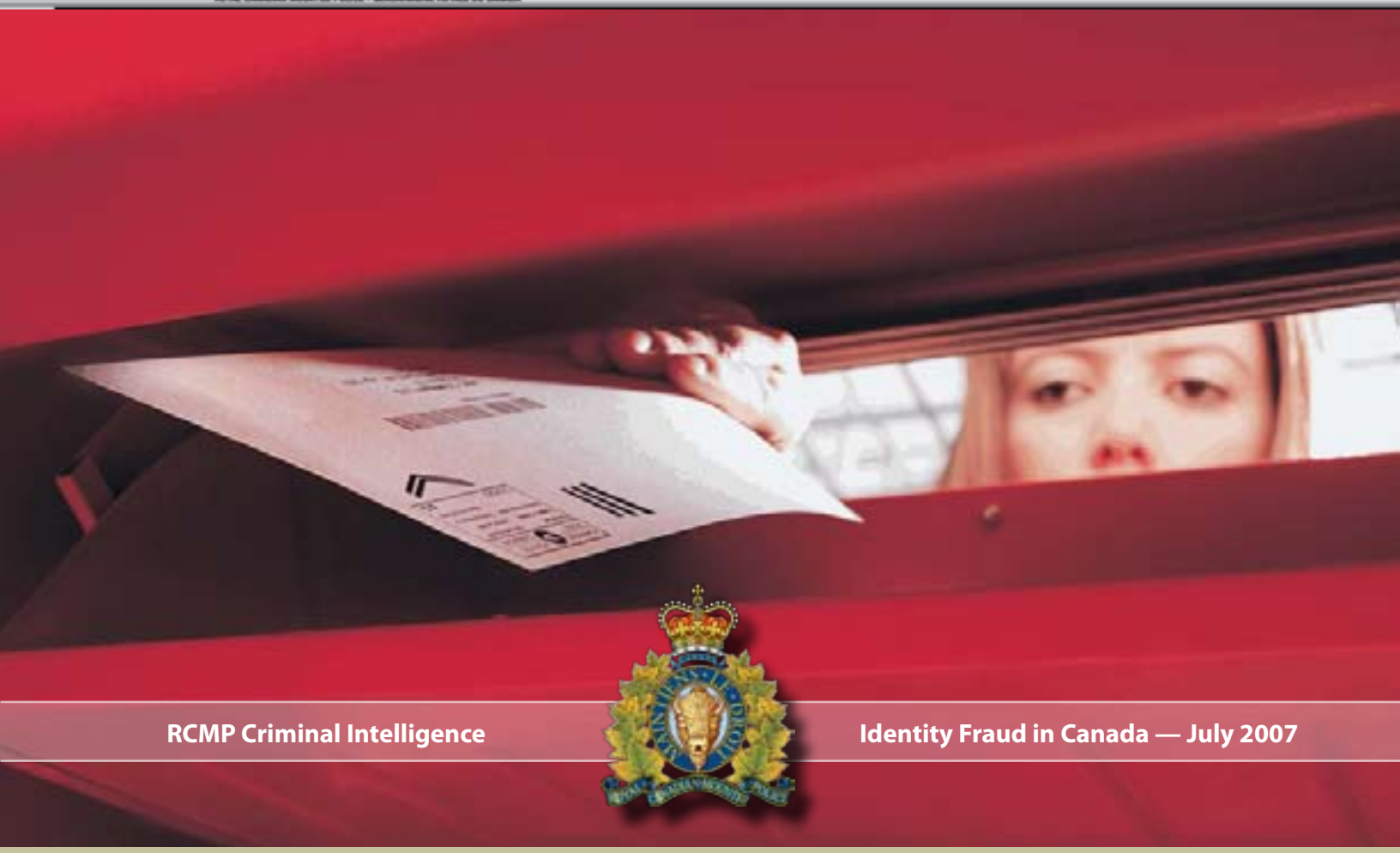
RCMP·GRC

ROYAL CANADIAN MOUNTED POLICE • GENDARMERIE ROYALE DU CANADA

Unclassified

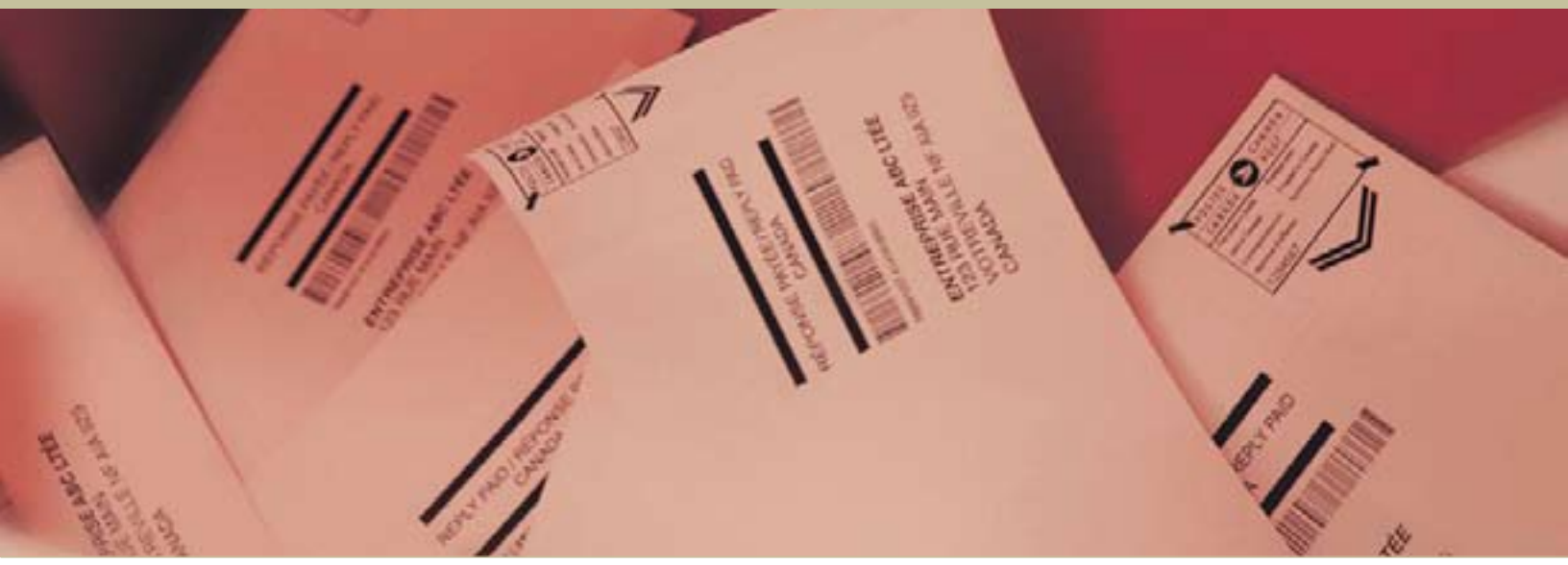


RCMP Criminal Intelligence

Identity Fraud in Canada — July 2007







Royal Canadian Mounted Police / Gendarmerie royale du Canada

Canada

Table of Contents

Executive Summary 1

Introduction 3

Identity Fraud Criminals in Canada 4

Organized Crime 4

Opportunists 4

Multiple Criminal Activities 5

Drug Trafficking 5

Mail Theft and Identity Fraud in the B.C. Lower Mainland 6

Methamphetamine and Identity Fraud 6

Immigration Fraud 8

Proceeds of Crime 8

Technology 9

The Internet and Identity Fraud 9

Victims 10

Youth 10

Geographic Scope 12

Rural Municipalities 12

National 12

International 12

Identity Fraud in Public and Private Sectors 14

Public and Private Sectors as Targets 14

Employee Corruption 15

Due Diligence 16

Client Service Versus Security 17

Table of Contents

Offences/Convictions 18

Phonebusters, The Canadian Anti-fraud Call Centre 19

Public Awareness/Education 20

Conclusion 21

Appendices

Appendix A — *Criminal Code of Canada* Offences used to Prosecute Identity Fraud 23

Appendix B — Glossary of Terms 24

EXECUTIVE SUMMARY

Identity fraud is a low-risk, high-profit criminal activity. As a result, conventional organized crime and other opportunists are increasingly involved. Personal information has become a valuable criminal commodity; trafficking in personal information and fraud using personal information without authorization are yielding significant profit for criminals.

Canadian public awareness of identity fraud increased as a result of two key events: the Ahmed Ressam terrorist plot as well as the 9/11 terrorist attacks in the United States. This report does not focus on terrorist activity associated with identity fraud.

The majority of cases this report documents reveal that criminals commit identity fraud to obtain financial gain. For many, a calculated benefit is the concealment of the criminal's true identity. The report also reveals criminals using or purchasing forged identification for the specific purpose of concealing their identities and/or prior convictions to facilitate criminal activity such as drug trafficking and immigration offences. True identity concealment presents investigative challenges to law enforcement.

Canadian identity fraud criminals live in both urban and rural areas, target their own neighbourhoods, travel to commit fraud, and target international victims. Criminals range from crude to extremely sophisticated, from one-person operations to organized crime. Some identity fraud criminals are indiscriminate in targeting victims while others choose victims based on factors such as their financial worth, residency status, ethnic background, vulnerability, or association to the criminal.

Of the nearly 200 investigations this report documents from 2001 through 2006, over 20 corrupt employees are identified. The majority are motivated by financial gain, however, debt repayment, and personal relationships are also identified as motivators.

Identity fraud is a global crime with a very personal impact. Even when victims are able to recover financial loss, they experience feelings of personal violation and may spend significant time restoring their personal and financial reputations. Some Canadian victims have been arrested or investigated by police because their personal information was used to facilitate criminal activity.

Canadian victims live in both urban and rural Canada. They are targeted by criminals who live in their neighbourhoods and are also the victims of provincial, national and international fraud schemes. Victims are individuals, living and deceased, businesses, corporations and government.

Compromised personal information is used to commit fraud immediately, stored for use at a later date and recycled by criminal groups. Once the target of identity fraud, Canadians have been victimized repeatedly.

Public and private sector entities are being targeted by criminals for the personal information they hold on clients and employees. Businesses are often wary to disclose personal information breaches because of the potential for negative repercussion such as loss of consumer confidence.

Mail theft is a common, effective and low-tech method used to acquire personal information on many individuals and businesses.

There is a strong link between methamphetamine use and identity fraud in British Columbia and Alberta. As methamphetamine use expands across Canada, it is probable that identity fraud crimes associated with meth use will also increase.

Forged, altered and genuine travel and other identification documents are the lifeblood of migrant smugglers and illegal migration in general. Migrant smuggling and the trafficking in documents to facilitate immigration crimes are lucrative criminal enterprises.

Technology has a large influence on the expansion of identity fraud crimes. Canadian identity fraud criminals, from low-level to high-level, use technology to facilitate their crimes. In addition, Canadians are targeted online by criminals in international fraud schemes.

ID fraud criminals make use of money service businesses to collect money from fraud targets, to exchange money for data with other criminals and to transfer illicit proceeds overseas. Profits range from petty cash to multi-million dollar schemes in which the proceeds of crime are, in some cases, never recovered.

Violence is an emerging threat associated with identity fraud crimes. As identity fraud crimes become more lucrative, they are attracting individuals/groups involved in violent crimes.

Identity fraud crimes have evolved. Current *Criminal Code* offences do not adequately address activity associated with the unauthorized acquisition, possession or trafficking of personal information with intent (payment card data and passports are the exception.)

Education and awareness strategies give people the tools needed to identify and prevent fraud schemes, which are constantly evolving. They do not, however, address or remove the responsibility from public and private sector institutions to exercise due diligence regarding personal information and personal information compromises.

Introduction

The following report is a national strategic intelligence assessment of identity fraud in Canada. It documents Canadian identity fraud investigations to identify the scope of the problem in Canada and to assess emerging and existing identity fraud trends.

The RCMP Commercial Crime Branch (CCB) requested this strategic assessment due to limited, national documentation and analysis of Canadian police identity fraud investigations.[1]

The RCMP CCB defines identity fraud as follows:

> *Identity fraud is the unauthorized acquisition, possession or trafficking of personal information, or, the unauthorized use of information to create a fictitious identity or to assume/takeover an existing identity in order to obtain financial gain, goods or services, or to conceal criminal activities.*

Investigations were submitted by the RCMP, provincial and municipal police services from 2001 to present. These cases should be viewed as a snapshot of identity fraud in Canada as it is estimated that annually, hundreds of Canadian law enforcement investigations comprise a component of identity fraud.

This assessment does not include payment card fraud as identity fraud unless personal information has been compromised in addition to credit or debit card numbers.

Information was collected primarily on criminals involved in acquiring, possessing or trafficking personal information for identity fraud purposes, manufacturing fraudulent I.D. or using personal information/forged I.D. to commit fraud. It links these criminals to organized crime involved in other criminal offences, such as drug trafficking or immigration offences, where applicable.

The terms *identity theft* and *identity fraud* are often used interchangeably. RCMP CCB uses the term *identity fraud* for two reasons. First, no adequate *Criminal Code* offences exist for the unauthorized acquisition, possession, or trafficking of personal information with intent, i.e. the "theft" aspect of the crime. Second, the vast majority of crimes committed using personal information without authorization involve fraud.

High-tech security expert Bruce Schneier contends that the term identity theft is misleading. He states, "Identity is not a possession that can be acquired or lost.... The real crime here is fraud — more specifically, impersonation leading to fraud.... No one's identity is stolen; instead, identity information is being misused to commit fraud.[3]

Examples of methods used to acquire personal information:	Examples of fraud committed using personal information without authorization:
Corrupt employees	Payment card fraud
Fraudulent mass marketing	Cheque fraud
Theft (mail, wallet)	Mortgage/title fraud
Break and Enters into residences, vehicles and businesses	Insurance fraud
Dumpster diving*[2]	Government program/service/benefit fraud
Phishing*, Pharming*, Spyware*	Government document fraud
Unauthorized access to computer	Immigration fraud
Mischief to data	Bank fraud (fraudulent accounts, account takeovers, loans)
Internet open sources	Account fraud (cell phones)
Social engineering*	Election fraud

1 For a broad, strategic overview of identity theft in Canada, the author recommends reading "Identity Theft: A Report to the Minister of Public Safety and Emergency Preparedness Canada and the Attorney General of the United States", Bi-National Working Group on Cross Border Mass Marketing Fraud, October 2004, http://www.psepc.gc.ca/prg/le/bs/report-en.asp

2 * See Appendix B — Glossary of Terms for all asterisked phrases.

3 Bruce Schneier, "Solving Identity Theft," *Forbes.com*, Security Matters, January 22, 2007.

Identity Fraud Criminals In Canada

Criminals recognize that personal information is a valuable criminal commodity. "Conventional" organized crime (OC) is therefore taking a greater interest in identity fraud as a criminal enterprise, not only to use fraudulent I.D. and aliases to conceal true identities and/or facilitate criminal activity.

Other criminal groups, such as street gangs and mail thieves in the B.C. lower mainland, are having a serious an impact on individuals, communities and corporations. Furthermore, many sophisticated conspiracies are directed by individuals with loose associations to other criminals, but would not constitute a criminal organization.

Investigators note that even the simplest criminal is computer-smart. Many have laptops with templates for numerous types of I.D. from multiple provinces. On their computers, they also store complete information profiles on numerous targets. The lack of sophistication of these criminals reinforces that the personal information of Canadians, wherever located, is easy to obtain.

Non-sophisticated techniques are also effective. Many investigations across the country reported that criminals store personal profiles on paper or in notebooks, which are easy to transport and leave no electronic footprint. Sometimes, low-tech and high-tech methods are used together. For example, groups gather personal information on targets both from mail theft and from hacking, or, individuals who store personal profiles in notebooks manufacture fraudulent I.D. documents using computers, software and other equipment.

Organized Crime

OC conceals criminal activity as a standard business practice. Use of fraudulently obtained or fictitious identities to register cell phones, to register companies, to purchase property, to lease vehicles, to conceal criminal records or to travel across borders is well documented.

Many criminal groups in Canada are involved in identity fraud. This includes, but is in no way limited to, Asian OC, West and East African Criminal Networks, Sri Lankan-based, Pakistani-based, Middle Eastern-based criminal groups and street gangs. As with OC in general, many criminal groups involved in I.D. fraud cannot be categorized in terms of ethnic origin.

Opportunists

Some opportunists identified in this report have made significant profit from their identity fraud activities. While it is difficult to classify I.D. fraud opportunists, some carve a niche market for themselves by providing services, such as document manufacturers or information procurers. Other criminals commit identity fraud purely for personal financial gain.

Some of the most sophisticated identity fraud criminals are individuals, not organizations. They also illustrates how easily one person can acquire thousands of pieces of personal information and defraud many individuals, organizations and government agencies. In terms of identity fraud, individuals can pose as great a threat as criminal organizations.

Multiple Criminal Activities

I.D. fraudsters are reported to have criminal histories that include fraud, forgery, Internet auction fraud, investment fraud, counterfeiting of money and credit cards, cheque fraud, kiting*, phishing*, and ATM fraud. Anecdotal information identified that currency counterfeiters are involved in forging identity documents. I.D. fraud criminals are also involved in many other non-fraud related criminal activities.

Drug Trafficking

There is a connection between methamphetamine use and/or addiction and identity fraud crimes which is covered in detail later in this section. Apart from this, a number of cases reveal links to drugs. This includes both drug trafficking by identity fraud criminals and by individuals who are operating using aliases/forged I.D.

Media reported that a mortgage broker in Vancouver was working in collusion with realtors to fraudulently purchase homes that were then used as marihuana grow operations. The broker and associates were reported to have falsified letters of employment for purchasers. It was believed that the names being used for the mortgage applications were new immigrants from the Vietnamese community who had no knowledge of the scheme.

Some employment letters included the home phone numbers of the brokers or of the real estate agent involved. In some of the real estate transactions, investigators were unable to verify the source of large down payments, sometimes of more than $100,000.[4]

This case suggests that criminals may have been laundering criminal proceeds to make down payments on homes that were then used to grow marihuana. The criminals' identities were protected because they were not listed as owners of the property. When they eventually sold the residences, they would make and additional profit on the property.

4 Kim Bolan, "100 grow-op houses found in mortgage scam probe," *Vancouver Sun*, Sept 25, 2004, p. A1.

Mail Theft and Identity Fraud in the B.C. Lower Mainland

A sub-culture of mail thieves and identity fraud criminals has evolved in the B.C. lower mainland in the past five years. This phenomenon is worth outlining in detail because of the serious impact it is having on individuals, communities and businesses in this region.

Mail theft is a low-tech and highly effective crime used to acquire personal information to commit identity fraud. Criminals in the B.C. lower mainland have become increasingly sophisticated, highly organized and their *modus operandi* (M.O.) is continuously evolving.

Methamphetamine and Identity Fraud

Health Canada reports that meth use in Canada has increased in recent years, particularly in Western Canada.[5] This correlates with investigations from British Columbia, Alberta and Manitoba that link meth use and identity fraud.

Mail thieves in the B.C. lower mainland use or are addicted to crystal meth. Some of the effects of this stimulant such as wakefulness, increased stamina and alertness, as well as the prolonged high of 4 to 12 hours[6] are conducive to the prolonged, repetitive tasks of breaking into mailboxes, sorting mail and creating identity profiles, dumpster diving* and testing credit cards online to see if they are active.

Police services in western Canada identified a link between meth use and an increase in crime in the region, including auto theft, weapons, identity theft and fraud.

This case demonstrates the drive, technological sophistication, international scope and evolution of the crimes committed by this meth/identity fraud ring. It reveals how easily personal information can be acquired, both locally and internationally. As with a significant number of I.D. fraud criminals, members of this group continuously re-offended.

The *RCMP Drug Situation Report 2005* identifies indicators of an increase in meth production in Canada:

- Organized crime involvement in the meth trade has led to an increased number of methamphetamine "super" labs; and
- Eastwardly expansion of methamphetamine production and distribution continued in 2005. In fact, the number of meth production sites in Ontario ranked second only to British Columbia.

The concern is that as methamphetamine production and use expands across Canada, identity fraud crimes associated with meth use and/or abuse will also increase.

5 Health Canada web site, "Be Drug Wise, Get the facts: methamphetamine", http://drugwise-droguesoisfute.hc-sc.gc.ca/facts-faits/meth_e.asp

6 Ibid.

Methamphetamine and Identity Fraud Case Study

A USA Today exposé tells the story of an Edmonton identity fraud ring that made substantial use of dumpster diving* behind banks, retail outlets, telecom companies, car rental agencies, restaurants and video rental stores, and at people's residences to find personal information to build personal profiles. The exposé reports that the fraud ring found data such as credit card transactions, loan applications, customer service reports, employee manuals, internal phone directories, credit profiles from credit reporting agencies, dates of birth and addresses.

The group was computer savvy and made use of Voice over Internet Protocol (VOIP) Internet phone services that permit the user to choose any area code, thereby, masking their location.

The group progressed to buying and selling personal information online in Internet Relay Chat channels with criminal groups in Quebec, Romania, Austria, and Egypt from whom it purchased identity profiles of American victims. The article reports that the Edmonton group would pay $200 USD for a profile that included a bank account password, credit card number with security code, Social Security Number, and then target these victims. The Edmonton group paid the other criminal groups with 'clean' money; money from ATM cash withdrawals which were then wired back to the crime group that supplied the profile. The Edmonton group also manufactured its own forged I.D. using computers, desktop publishing software and I.D. templates. It would test and exploit financial web sites such as e-mail cash transfers offered by some Canadian banks.[7]

7 Byron Acohido and Jon Swartz, "Meth addicts' other habit: Online theft," *USA Today*, December 15, 2005.

Immigration Fraud

Forged, altered and genuine travel and other identification documents are the lifeblood of migrant smugglers and illegal migration in general. The involvement of organized crime in migrant smuggling and in the manufacture of forged identification for illegal immigration purposes is well documented globally.

Identity fraud crimes associated with immigration offences will continue to increase as Canada is a choice destination for immigrants seeking a better quality of life. In addition, migrant smuggling and the trafficking in documents to facilitate immigration crimes are lucrative criminal enterprises.

Fraudulent affidavit created by main target in US Treasury bond case

Proceeds of Crime

The majority of identity fraud criminals this assessment evaluates are motivated by financial gain. Profits range from petty cash to multi-million dollar schemes in which the proceeds of crime are, in some cases, never recovered. In many cases, in particular those investigating the theft of personal information, financial losses are unknown.

In cases where financial gain is the goal, payment card fraud (mostly credit card fraud) is documented more than any other type of fraud. Bank account fraud is also frequently reported. In comparison, a much smaller number of mortgage frauds are reported, however these frauds net significantly more money ($100,000 +) in a single transaction.

Money Service Businesses

Criminals commonly make use of money service businesses to collect money from fraud targets in mass marketing schemes. This M.O. is reported in most mass marketing cases submitted to this assessment.

Identity fraud criminals actively exchange and/or purchase personal information through the Internet. Often, profits from personal information exchanges are shared with all parties involved. Money service businesses are used for some of these financial transactions.

Targeting the criminal proceeds in identity fraud cases could be a strong deterrent to these criminals. This view is supported by a number of identity fraud investigators who contributed to the assessment.

TECHNOLOGY

Canada is one of the most wired countries in the world with a highly technology-literate population. Canadian criminals are technologically sophisticated and take advantage of Canada's wired infrastructure to facilitate identity fraud. International criminals take advantage of this infrastructure to target Canadians for identity fraud. Some schemes are extremely sophisticated while others are simple, yet effective.

Hackers are profit-motivated criminals. It also demonstrates that international computer crime investigations are complex, involve law enforcement in multiple jurisdictions and often meet with mixed success.

The Internet and Identity Fraud

The Internet hosts many web forums devoted to identity fraud. Increasingly, personal information is traded and sold online in restricted web sites, via instant messaging and in chat rooms. The following investigation provides an example of the broad scope of criminal activity on carder* web sites.

Operation FIREWALL[8, 9]

In 2004, an international US-led investigation identified three "computer underground criminal groups": Shadowcrew, Carderplanet and Darkprofits. The groups operated websites used to traffic counterfeit credit cards and false identification information and documents. These websites shared information on methods used to commit fraud, and also provided a forum by which to promote and facilitate the electronic theft of personal identity information, payment card fraud, and the production and sale of false I.D. documents.

Three individuals, two from the US and one from Russia, administered the Shadowcrew website by controlling who became members and moderators. The indictment alleges that these three were responsible for the overall Shadowcrew "marketplace".

After initial contact via the Internet, the suspects exchanged stolen information and counterfeit identification documents such as credit cards, driver's licenses, domestic and foreign passports, and birth certificates. The website had nearly 4000 members.

Twenty-eight people were arrested in eight US states and six countries. The group is estimated to have trafficked 1.7 million stolen credit card numbers, and financial institutions approximated losses at more than $4.3 million.

8 U.S. Secret Service Press release, GPA-23-04, "U.S. Secret Service's Operation Firewall Nets 28 Arrests; International Undercover Investigation Prevents Millions in Financial Loss," October 28, 2004.

9 US Department of Justice ,"Nineteen Individuals Indicted in Internet 'Carding' Conspiracy; Shadowcrew Organization Called 'One-Stop Online Marketplace for Identity Theft," Oct 28, 2004

The Internet facilitates I.D. fraud. Criminals have access to massive amounts of personal information from legitimate sources, or through the criminal online trade in data. The Internet facilitates criminal anonymity, as well as the ability to appear legitimate, as phishing cases demonstrate. The Internet also provides criminals with access to hundreds or thousands of potential victims via spamming/phishing.

Technology complicates investigations. Investigations involving the Internet or electronic data require the timely forensic analysis of computers and other devices. Often, potential evidence cannot be retrieved. Many become multi-jurisdictional investigations that often cross international boundaries.

VICTIMS

People are the true victims of identity fraud. The personal information criminals seek is both random, in the case of large corporate thefts, and targeted towards specific communities, wealthy individuals, family members and people who are vulnerable such as youth, those in need of money or with mental disabilities.

Most of the time, victims discover that their personal information has been breached following a fraud. For example, they receive bills for goods and services that they did not purchase, phone calls related to credit applications, they are denied credit, they discover empty bank accounts, they apply for a passport and one has already been issued to another person in their name or they receive notice that payments are due on mortgages for homes that they have owned for years.

Most victims are responsible to restore their financial reputation on their own. This is a time consuming, frustrating process that often involves conflict with institutions and is limited in success. Some police investigating identity fraud have assisted victims in dealings with uncooperative institutions.

Financial institutions reimburse money to individuals who are the victims of payment card fraud and account takeovers. These institutions often do not consider reimbursed individuals to be true victims since they are financially compensated for their losses. Furthermore, individuals are rarely told where or how a breach has taken place due to the institution's ongoing investigation. Withholding this information can contribute to a victim's sense of alienation and violation.

For victims, losses are not just monetary, but personal. Along with feeling alienated or violated, victims may feel fear, hopelessness and harassment. In addition, people whose credit histories are tainted as a result of ID fraud can be denied employment or security clearances.

Once a person has been a target of identity fraud, they can be victimized repeatedly over time. Therefore, it is important that individuals notify all relevant agencies, including credit bureaus. It is ***critical*** that victims file a police report following any fraud committed in their name to create an official record to protect themselves. Identity fraud victims have been investigated and arrested in Canada following crimes committed in their name.

Youth

Youth are viewed as an emerging group that will increasingly become the target of identity fraud. This is due to pristine credit ratings, a proliferation of personal information available on the Internet, and youth possessing an increasing number of security documents.

Internet

Youth are prolific users of Internet chat rooms, instant messaging and, more recently, social networking sites. Social networking sites such as MySpace, Friendster and Facebook are virtual communities where individuals develop personal profiles by posting photos and personal information, by linking their profile to other profiles thereby developing a network of friends, and then by cross-posting to the sites of their

friends. The information they post can be as narrow or as broad as they choose. "We have to start with the premise that (social networks) are here to stay. We also have to start with the premise that they're socially useful, fun and have benefits." [10]

From a law enforcement perspective, youth posting personal information to the Internet increases the risk of luring by child predators. Coupled with information available on youth from other on-line sources, identity fraud should be an additional concern.

Canadian security documents

Children are also vulnerable to identity fraud because they possess multiple Canadian security documents at an earlier age. For example, to benefit from Canadian benefit programs such as the Registered Education Savings Plan, children require a SIN. Since 2004, Canadian children require their own passport to travel abroad. Prior to 2004, the names of minor children could be inserted on a remarks label affixed to the visa pages of the parents' passports. The new policy is in place to combat the human trafficking of children.[11] While the issuance of government identification to children prevents certain types of fraud and other serious crimes against children, ironically, possession of multiple pieces of government I.D. increases children's vulnerability to identify fraud because their personal information resides in more physical and electronic locations.

10 Parry Aftab, executive director WiredSafety.org, Shannon Proudfoot, "Taking back MySpace," *The Ottawa Citizen*, May 11, 2006

11 http://www.passportcanada.ca/ombudsman/omb-ar2005-06.aspx?lang=e

Geographic Scope

Identity fraud is a global crime with a very personal impact. Many crimes are committed locally and have a substantial, negative impact on the local community they target. Of interest, the majority of cases identified in this assessment had connections in two or more provinces and/or international connections.

Rural Municipalities

Identity fraud is not an urban phenomenon. Some identity fraudsters, in fact, target smaller communities where they suspect they can evade detection.

A number of cases reported victims in small communities whose personal information had been used in large urban areas, often in other provinces. Few victims knew the source of compromise of their personal information.

National

Many I.D. fraud victims reside in a different province from the crime and/or perpetrators. Victims discover that their personal information has been used in other provinces to forge identity documents, to acquire services (cellphone and other), through the loss of money from bank accounts, credit cards and mail re-routing. They discover the compromise when they receive phone calls, bills for service, access accounts or attempt to apply for services/Canadian security documents.

Suspects residing in one province intentionally travel to a separate/multiple provinces to commit fraud. Suspects frequently have a history of criminal activity in their province of residence and, therefore, commit fraud in other jurisdictions to minimize detection and/or penalties.

International

Many I.D. fraud investigations throughout this report have an international link, whether it be criminal associates, targets, technology or immigration-related.

Canadian fraudsters target victims in other countries. A number of investigations involve mass marketing fraud (lottery scams, advanced fee fraud scheme, government rebate fraud, loan scheme) primarily targeting US citizens. Victims are asked to cash cheques (legitimate stolen cheques which were counterfeited) or counterfeit bank drafts, keep a portion of the proceeds and wire funds back to the fraudster. When cheques bounce, victims are responsible for the funds. In many of these cases, fraud artists request and receive personal information from victims, including bank account information, which the fraudsters then use to withdraw funds from the victims' bank accounts.

Canadians are also the target of mass marketing fraud schemes by international criminals.

Identity fraud has no boundaries. Canadians who live in rural municipalities are as vulnerable to identity fraud schemes as individuals in large urban cities. They are targeted by criminals operating locally, across Canada and internationally. This is faciliated by the fact that everyone's personal information resides in public and private databases that can be breached across Canada. In addition, our wired infrastructure means that identity fraud criminals who live in or outside of Canada can target anyone via the Internet, regardless of where they live.

Identity Fraud in Public and Private Sectors

Public and private sector institutions are increasingly targeted by identity fraud criminals for their client and employee data. This report also identifies that they are not exercising required due diligence to protect themselves and client personal information from this threat.

Public and Private Sectors as Targets

Canadian businesses, public and private sector institutions are being targeted by identity fraud criminals for the theft of personal information of employees and clients as well as equipment and blank documents. Criminals are both internal and external. Breaches are committed by corrupt employees, through the electronic theft of data and through the physical theft of data.

Personal information breaches range from small companies with breaches of several employees' and/or clients' information, to large institutions with breaches affecting thousands of clients. The impact of a small breach of client data from a small company can be as devastating to a business' operations and reputation as a large breach at a large corporation or public institution.

As most identity fraud criminals are motivated by financial gain, arguably, financial institutions are the largest corporate victims of identity fraud. They are targeted both for their client information and for money in loan schemes, payment card fraud, bank account fraud and mortgage fraud.

Payment card fraud

Payment card fraud (primarily credit card fraud) was committed more than any other type of fraud associated with identity theft. This includes fraudulent applications, the use of credit cards and the manufacturing of forged payment cards. In these cases, payment cards were linked to identity fraud in some way.

Criminals recognize that credit card fraud is lucrative and easy to commit. Credit card numbers are easy to acquire through mail theft, skimming operations or on online carder* sites. Applications are readily accepted by financial institutions and merchants, whether in person or on-line, rarely ask for supporting I.D. or perform other security checks.

Cheque fraud

Some police services have has seen a recent proliferation of cheque fraud. Corporations are victimized by criminals who steal and forge corporate cheques and letterhead which are used in numerous mass marketing and other criminal schemes. Legitimate cheques are primarily retrieved through mail theft. Manual/physical examination is required to counteract forging techniques. The quality of forged cheques is improving and often beat standard 5 to 10 day holds.

Forged corporate cheques have been found in labs that also forge I.D. Scanned corporate cheques have been found on the laptops of I.D. fraud criminals.

Theft of equipment and blank documents

Blank identity documents and equipment used to manufacture I.D. are valuable assets to I.D. fraud criminals. Businesses and institutions in possession of them should handle and store them as a valuable asset.

Identity fraud criminals have targeted hospitals to steal card embossers which are used to manufacture forged identification.

> *In 2005, a Stonewall, Man. insurance agency was the victim of a "professional" B&E, according to RCMP interviewed by the media. The thieves stole computer equipment, a camera, hundreds of blank photo I.D. cards and the backdrop used take photos for driver's licences.*[12]

> *The media reports that in September 2005, break and enters at two provincial Ministry of Health Vital Statistics offices, one in Victoria and the other in Vancouver, occurred within hours of each other. Authorities believe that this was a coordinated operation. One thousand blank birth, death and marriage certificates were stolen. Police stated that criminals knew which cabinet the certificates were stored, which could indicate insider collusion.*[13]

Non-targeted breaches

Other breaches may or may not be targeted, but still put client data at risk.

> *CIBC issued a news release that in Montreal on January 2007, Talvest Mutual Funds, CIBC Asset Management announced that a backup file containing "information relating to the processes used to open and administer approximately 470,000 current and former Talvest client accounts" had gone missing in transit between its offices. The file may have included client names, addresses, signatures, dates of birth, bank account numbers, beneficiary information and SINs. The news release stated that the company was notifying all clients by letter and would be responsible for any monetary loss arising from this breach.*[14]

Corporations cannot turn a blind eye to the fact that the personal information they possess is of value to criminals. Threats come from within and outside corporations. In view of this threat, corporations must re-evaluate their security practices at all levels (personnel, data storage, data access, third-party contracts with access to data) to mitigate the risk of loss of client data.

Employee Corruption

Corruption within public and private institutions undermines public and economic trust in these institutions. Corruption exists when an employee uses his/her position of employment to acquire, possess or traffic employee or client information without authorization and/or uses his/her position of employment to commit fraud.

Motivation

Most employees in public and private sectors were motivated by financial gain.

Links to OC

Corrupt employees at government agencies can build a reputation as a service provider to criminals.

Employers need to be aware of the value of personal information to criminals, the motivators of corrupt employees and indicators that an employee could be corrupt to decrease the threat of compromise to client and employee data.

12 Adam Clayton, "Mounties fear theft done for id fraud: License gear stolen," *The Winnipeg Sun*, 2005-04-10, p. A5.
13 David Carrigg, "ID-theft ring suspected in twin break-ins," *The Province*, September 16, 2005.
14 CIBC Corporate News Release, "Talvest Mutual Funds issues statement regarding missing back up computer file," Montreal, January 18, 2007.

Due Diligence

Whereas public and private sector institutions are being targeted for identity fraud, many are vulnerable because they do not practice due diligence. This includes secure hiring and personnel security procedures, secure storage and transmission of sensitive client and employee data, and protection/verification of other assets. In general, security considerations are secondary for profit-motivated industries. Often, corporations are hesitant to funnel resources into security measures unless there is the potential for financial loss.

In 2006, mortgage fraud raised public outrage Ontario in view of the fact that Ontario law and court decisions gave greater rights to lending institutions than homeowners who had been defrauded of the title on their properties and were deemed responsible for mortgages as a result of the fraud. An October 2006 decision by the Superior Court of Ontario sided with the rightful property owner and, in cases where the lending institution does not exercise due diligence, it is responsible for the mortgage fraud loss.

This particular case involved fraudsters posing as the legitimate owners and a fraudulent purchaser presenting forged identification documents to a lawyer who, unknowingly, facilitated the transfer of title and transaction with the lending institution. When the fraud was discovered, the rightful owners and bank agreed that the couple be declared the rightful owners, but disagreed who was responsible to repay the mortgage.

The court ruled that the bank had not exercised due diligence. It failed to detect signs of fraud in failure to convey parking and storage spaces, payment of $30,000 to the mortgage broker for a standard mortgage, and the absence of a deposit being paid. Of greatest impact, the lending institution did not send an appraiser to the property, which, the judge stated, "would have uncovered the fraud." [15]

In December 2006, The Ontario Government passed the *Consumer Protection and Service Modernization Act, 2006*. The Act (1) ensures that rightful owners will not lose property as a result of the registration of a falsified mortgage, fraudulent sale or a counterfeit power of attorney, (2) streamlines the Land Titles Assurance Fund so that in standard cases of fraud, title is returned and a decision on compensation made within 90 days, and; (3) increases fines for real estate fraud from $1000 to $50,000.[16]

Property laws are provincial jurisdiction therefore laws governing mortgage and title fraud vary in each province.

Security Breach Disclosure Legislation

In most cases, institutions are not the owners of a client's personal information — they are merely custodians. Frequently, breaches of client data are not reported to clients or to law enforcement because of the potential for negative repercussions such as a loss of client base, devaluation of stock, or costs associated with disclosure and securing the vulnerability. Furthermore, there is no mandatory public disclosure in Canada.

Currently, notification of personal information breaches remains a corporate decision in Canada. In the United States, many states have enacted security breach disclosure legislation. Individuals who are notified that their personal information has been breached can take steps to prevent the use of this information for fraud. The lack of control/helplessness that victims feel has been well documented in identity fraud cases; this is one way that they can regain some control. In addition, mandatory public disclosure requirements can motivate institutions to better protect personal information in their possession.

This lack of legislation was recently publicized following the January 2007 breaches of client credit card information from Winners and HomeSense and a missing back-up file containing 470,000 client from Talvest Mutual Funds. Security breach investigations undertaken by the Office of the Privacy Commissioner, such as that into Talvest Mutual Funds, are not legally binding can only offer recommendations for change.[17]

15 Ontario Superior Court of Justice; Rabi v. Rosu, 2006 CanLII 36623 (ON S.C.), 2006-10-31, 06-CV-311147

16 "Real estate fraud gives homeowners peace of mind," Queen's Park, February 5, 2007. www.gov.on.ca/MGS/en/News/112294.html

17 Michael Geist, "Identity theft in Canada," www.p2pnet.net/story/11084, 2007-01-22

Client Service Versus Security

In today's fast-paced, technologically advanced society, there is constant pressure to ensure that services are rendered as quickly, easily and as cost-effectively as possible. Examples include trends towards online applications for Canadian security documents, government benefits and online banking transactions.

In contrast, increased security measures to protect data, personal information or to ensure document integrity require time, resources and can be costly. Often, security practices are assessed and implemented using risk management principles; institutions assess the potential for loss as well as costs to their operation associated with varying degrees of security.

Client service and security requirements are in clear opposition. Client service aims to fulfil client requests, such as the issuance of credit or identification, as quickly and with minimal burden on the client whereas security aims to eliminate risk, which is usually more costly, timely, and burdensome on the client. The ultimate challenge is finding a balance.

Offences/Convictions

Identity fraud is viewed as a victimless crime with few penalties because often it does not involve violence and because financial institutions reimburse victims for most financial losses. Low penalties are not a deterrent given the high profits involved. As a result, there is an extremely high recidivism rate among identity fraud criminals. A number of suspects are career criminals or have lengthy criminal records.

Identity fraud crimes are prosecuted using many *Criminal Code of Canada* (CCC) offences. A non-exhaustive list of 46 offences compiled for the assessment is provided in Appendix A. No adequate CCC offences exist for the unauthorized acquisition, possession or trafficking of personal information with intent (payment card data and passports are the exceptions.)

In data received for the project, sentences ranged from 6 years and subsequent deportation to no conviction. The 6-year sentence was a severe penalty for a Canadian identity fraud case.

The most common punishment for corrupt employees was firing, which often had taken place before police were asked to investigate. In at least nine cases, employees were charged. In most cases, insufficient data was provided to the project to follow up on these charges.

There is insufficient data to further assess charges and convictions as many convicted fraudsters had not been sentenced at the time of collection, some cases were still under investigation, or data was not reported/unavailable.

PhoneBusters, The Canadian Anti-fraud Call Centre

PhoneBusters, "The Canadian Anti-fraud Call Centre" is the central agency in Canada that collects and collates complaint information on mass marketing, advanced fee fraud letters (Nigerian letters) and identity theft complaints. The information is disseminated to the appropriate law enforcement agencies on a priority basis. The data collected at PhoneBusters is a valuable tool in evaluating the effects of various types of fraud on the public. It also helps to prevent future similar crimes from taking place. This national anti-fraud call centre is operated by the Ontario Provincial Police (OPP) in partnership with the RCMP and the Competition Bureau.[18]

Reporting Economic Crime Online (RECOL) is an online initiative that permits individuals to report economic crimes and people register their complaints online. The service is administered by the RCMP and partnered with the OPP and the US-based Internet Fraud Complaint Center. [19]

PhoneBusters and RECOL are in the process of merging operations under The Canadian Anti-Fraud Call Centre.

PhoneBusters already has in place a network of Canadian and international law enforcement and private sector partners. The centre provides investigative leads to law enforcement across the country as well as statistical and tactical reports on identity fraud in Canada.

18 www.phonebusters.com/english/aboutus.html
19 www.recol.ca

Public Awareness/education

Public awareness and education are key to reducing identity fraud. Canadian law enforcement, public, private and volunteer sectors are involved in many fraud-prevention initiatives aimed at educating people to minimize their risk of becoming the victims of fraud. However, identity fraud victims continue to be responsible to restore their financial and personal reputations.

Education is a key component of PhoneBusters. Each individual who contacts the call centre to report a scam/victimization receives information to reduce/minimize the risk of additional compromise.

"Fraud: Recognize it. Report it. Stop it." is an anti-fraud slogan created in 2005 by the Fraud Prevention Forum (FPF). The FPF, chaired by the Competition Bureau, is a concerned group of private sector firms, consumer and volunteer groups and government and law enforcement agencies committed to fighting fraud aimed at consumers and businesses. It works to prevent Canadians from becoming victims of fraud through education. Approximately 90 entities participate in this partnership.[20]

The FPF has designated March as Fraud Prevention Month in Canada. The objectives of this annual campaign are to:

- deliver messages that will educate the public about fraud,
- help Canadians avoid becoming victims and encourage reporting,
- build awareness on the scope and pervasiveness of consumer and business fraud in Canada, and;
- make Canada a hostile environment for these crimes.

Coinciding with the launch of fraud prevention month in 2007, the RCMP Commercial Crime Branch released "Personal Information and Scams Protection — a Canadian Practical Guide." This guide focuses on the protection of personal information, outlines numerous fraud scams, highlights red flags or indicators that could signify fraud and provides readers with practical tools and links to reduce their risk of becoming fraud victims. This fraud prevention tool builds on its successful predecessor, the Student Practical Guide, and is available on the RCMP web site at www.rcmp-grc.gc.ca/scams/canadian_practical_guide_e.htm#mail.

Education and awareness strategies give people the tools needed to identify and prevent fraud schemes, which are constantly evolving. These strategies allow people to take control and to better protect personal information by questioning the need to supply personal information to requesters (i.e. postal codes to retailers), by teaching to shred documents and by informing of personal information that should not be kept in wallets, for example.

Education and awareness do not, however, address or remove the responsibility from public and private sector institutions to exercise due diligence regarding personal information and personal information compromises.

20 www.fpf.ca

Conclusion

This assessment demonstrates that personal information has become a valuable criminal commodity. The disturbing reality is that in the electronic age, we have lost track of all of the locations in which our personal information resides. Public and private sector institutions as well as individuals therefore need to handle and protect information with these facts in mind.

Public and private sector businesses and/or institutions must be sensitized to the criminal value of the personal information they possess and assess their security practices at all levels (personnel, data storage, data access, third-party contracts with access to data) to mitigate the risk of loss of client and employee data. Threats are both internal and external.

The investigation of identity fraud crimes requires multiple partners from law enforcement, government and the private sector due to the scope and nature of these crimes. Investigations identified in this report with multiple, cooperating partners met with the greatest success.

Canada does not want to emerge as a haven for international identity fraud criminals, yet low criminal penalties and significant profits reaped from identity fraud schemes place the country at risk.

In addition, victims currently harbour the majority of responsibility to restore their financial and personal reputations.

Many fraud investigators and analysts contend that identity fraud and other financial crimes are of low priority within law enforcement and criminal justice communities. Organized crime, terrorism, drug trafficking and violent crimes all receive priority. Yet, identity fraud facilitates all of these crimes.

Of great concern, identity fraud crimes pose an immediate and severe threat to the integrity of our public and private institutions: to name a few, banks, postal institutions, government departments and credit bureaus are all being targeted and compromised. Victims of identity fraud lack trust in these institutions. They question our inability as a society to protect individuals from and properly address identity fraud crimes. Until the global scope and personal impact of identity fraud is understood, it will not be viewed as a serious crime.

To quote The Honourable Judge S.C. Antifaev:

The possession of the credit cards, possession of the identification, the alteration of the drivers' licences, not just once but twice on the last occasion, the possession of the forged Canada Post mail key are extremely serious offences.... This is, unfortunately, the kind of behaviour that, if it is not met sternly by the court, is going to result in the public having a complete lack of faith in its mail system and a complete lack of faith in the validity of the drivers' licensing system, and a lack or a lessening of faith of the public and people in the financial field of the validity of documents that we all take for granted, that we all rely on every day. I am referring to not only our identification, but our bank cards, our credit cards and documents of that nature. These are crimes that go to the root of how people live in our society. Unless these crimes are checked in a serious way, unless the courts and others deal very seriously with these types of offences, which frankly are identity-theft offences, it will lead to a weakening of the whole social fabric that we all rely on.

R. v. Brian Christopher McNeil, 2006–01–25
Provincial Court of British Columbia

Appendix A — CCC Offences Used to Prosecute Identity Fraud

Offence	Statutory Provision
Forgery of or uttering forged passport	Criminal Code s. 57. (1)
False statement in relation to passport	Criminal Code s. 57. (2)
Possession of forged, etc., passport	Criminal Code s. 57. (3)
Fraudulent use of certificate of citizenship	Criminal Code s. 58. (1)
Breach of trust by public officer	Criminal Code s. 122
Failure to comply with condition of undertaking or recognizance	Criminal Code s. 145 (3)
Theft, forgery, etc., of credit card	Criminal Code s. 342.(1)
Unauthorized use of credit card data	Criminal Code s. 342.(1) (3)
Making having or dealing in instruments for forging or falsifying credit cards	Criminal Code s. 342.01 (1)
Unauthorized use of computer	Criminal Code s. 342.1 (1)
Possession of property obtained by crime	Criminal Code s. 354. (1)
Theft from mail	Criminal Code s. 356. (1)
False pretence or false statement	Criminal Code s. 362. (1)
Forgery	Criminal Code s. 366. (1)
Making false document	Criminal Code s. 366. (2)
Uttering forged document	Criminal Code s. 368. (1)
Exchequer bill paper, public seals, etc.	Criminal Code s. 369
Counterfeit proclamation	Criminal Code s. 370
Telegram, etc., in false name	Criminal Code s. 371
False messages	Criminal Code s. 372 (1)
Drawing document without authority, etc.	Criminal Code s. 374
Obtaining, etc., by instrument based on forged document	Criminal Code s. 375
Counterfeiting stamp, etc.	Criminal Code s. 376. (1)
Counterfeiting mark	Criminal Code s. 376. (2)
Damaging documents	Criminal Code s. 377. (1)
Offences in relation to registers	Criminal Code s. 378
Fraud	Criminal Code s. 380. (1)
Using mails to defraud	Criminal Code s. 381
Fraudulent registration of title	Criminal Code s. 386
Fraudulent sale of real property	Criminal Code s. 387
Misleading receipt	Criminal Code s. 388
Disposal of property to defraud creditors	Criminal Code s. 392
Fraudulently obtaining transportation	Criminal Code s. 393 (3)
(Falsification of) Books and documents	Criminal Code s. 397. (1)
Falsifying employment record	Criminal Code s. 398
False return by public officer	Criminal Code s. 399
Personation with intent	Criminal Code s. 403
Personation at examination	Criminal Code s. 404
Acknowledging instrument in false name	Criminal Code s. 405
Forging trade-mark	Criminal Code s. 406
Passing off	Criminal Code s. 408
Instrument for forging trade-mark	Criminal Code s. 409. (1)
Other offences in relation to trade-marks	Criminal Code s. 410
Unlawful use of military uniforms or certificates	Criminal Code s. 419
Mischief in relation to data	Criminal Code s. 430.(1.1)

Appendix B — Glossary of Terms

Carder:

A criminal who engages in carding, a form of identity theft. Carders use lists of credit and debit card information to perpetrate multiple acts of fraud by making purchases without the consent of the original card holder.

Dumpster diving:

Sifting through commercial or residential garbage to find usable items; in this case, information.

Card embosser:

This equipment is used to add digital information to plastic card magnetic strips.

Internet Protocol (IP) address:

A unique number that devices use in order to identify and communicate with each other on a network utilizing the Internet Protocol standard.

Kiting:

Cheque kiting involves drawing money from a bank account that does not have sufficient funds to cover the cheque.

Keystroke Logger:

Hardware devices or software applications which capture a user's keystrokes.

Malicious Code/Malware ("malicious software"):

A program deliberately designed to capture/modify/damage data or change a computer behavior without the user's explicit knowledge or intention. Malware includes Trojan horses, spyware, viruses and worms.

Personal Information:

For the purpose of this document, personal information refers to any element or combination of information that can normally be used to uniquely identify an individual in the delivery of goods and services, government services or law enforcement activities. Alternatively, it can also designate information to be used to acquire additional information on someone.

Phishing:

Pronounce "fishing". It is the use of social engineering in electronic messaging to provoke an immediate impulsive reaction from individuals into visiting fraudulent websites. The ultimate goal is to acquire personal or sensitive information.

Social Engineering:

The practice of manipulating someone's trust for the purpose of gaining some advantage.

Spam:

Unsolicited or undesired bulk electronic messages.

Spoofing:

Modification of identification or authentication information to mislead the reader on the true identity of the originator.

Tombstone data:

The personal information of deceased individuals which is used by forgers to impersonate or assume the identities of the deceased individuals to commit fraud.[21]

21 Definitions taken from the RCMP CCB "Personal Information and Scams Protection - a Canadian Practical Guide." and wikipedia.org.

Notes

RCMP Criminal Intelligence

Identity Fraud in Canada