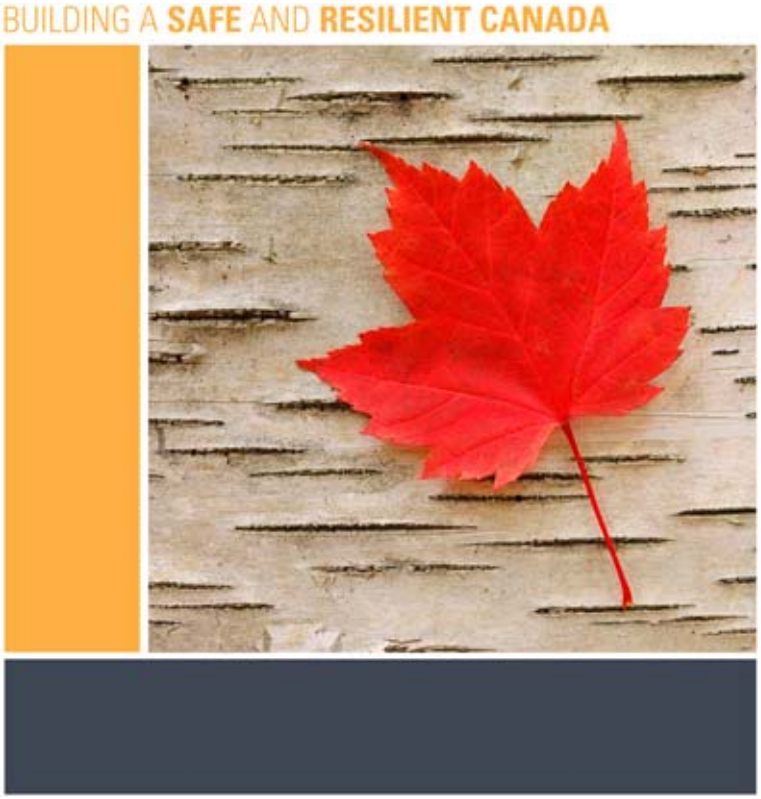
Public Safety Canada | Sécurité publique Canada



Public Safety Canada
Measuring the Extent of Cyber-Fraud in Canada
A Discussion Paper on Potential Methods and Data Sources

AUGUST 2011
RDIMS #465951

Canada

Measuring the Extent of Cyber-Fraud: A Discussion Paper on Potential Methods and Data Sources

Sara M. Smyth
Simon Fraser University

and

Rebecca Carleton

prepared for

Research and National Coordination
Organized Crime Division
Law Enforcement and Policing Branch
Public Safety Canada

The views expressed herein are those of the authors and do not necessarily reflect those of the Department of Public Safety Canada.

Report No. 020, 2011

Cat. No.: PS14-4/2011E-PDF
ISBN No.: 978-1-100-19193-5

Table of Contents

Executive Summary

Central to developing and monitoring the progress of strategies for combating cyber crime is reliable information about crime volume, in terms of the number of incidents and offenders, the prevalence of cyberspace tools for the commission of crime, as well as the number of victims. This discussion paper assesses the potential for using innovative methodologies to estimate the scope of cyber-fraud, identifies existing data sources and gaps, and suggests novel sources of data that may help provide a more accurate picture of the degree of cyber-fraud in Canada. Further, possible ways to determine the proportions of cyber-fraud attributable to criminal networks rather than single individuals are discussed. This research is informed by a literature review and interviews with law enforcement and Information Technology (IT) personnel.

The literature review and interviews show that the largest impediment to effectively managing the problem of cyber-fraud is the lack of reliable data. The Government of Canada primarily relies on police-reported data for information about cyber-fraud. Yet, there are a number of reasons why fraud incidents are not reported to police. For example, companies may prefer to handle such matters internally, or individuals may only report that they were defrauded to their financial institution.

This research shows that current information about cyber-fraud is being funnelled to a variety of different organizations, including banks, regulatory agencies and various police agencies, or is simply not recorded. There is a clear shortage of data measuring the prevalence and costs of cyber-fraud in Canada and the available information is incomplete and fragmented. The lack of reporting of cyber-fraud incidents by individual and corporate/government victims means that many cases are not recorded or represented in official crime statistics This research demonstrates a strong need for the creation of a national centre to record and measure data relating to cyber-fraud across Canada. A central databank of known cyber-fraud offenders and cases across the country could facilitate the identification and tracking of suspects in cyber-fraud cases and could further understanding regarding when one individual, or group of individuals, is committing fraud all over the country. Ultimately, a national databank on cyber-fraud incidents could give law enforcement officials a better understanding of the types of cyber-fraud being committed in Canada.

Sophisticated technologies and the global distribution of computer networks also increase the difficulty of detecting and addressing cyber-fraud and hinder the ability to find and prosecute criminals operating online. In addition, there are operational challenges related to ensuring that law enforcement officials have the training and resources they need to adequately address the problem and able to identify perpetrators of cyber-frauds. Attempting to locate a perpetrator is problematic in many cases of cyber-fraud because skilled attackers cover their tracks by using proxies and other technical obfuscation methods.

This research suggests that the best source for further information on cyber-fraud is offender populations. Offender interviews may help uncover the network structure of hidden populations and help the law enforcement community to identify key players within the group. Of the options available for hidden populations, a truncated Poisson model is suggested as the most effective model. Ideally, this research could help pave the way for data collection and analysis that would

better inform law enforcement officials, investigators, and policy makers about the extent of cyber-fraud and cyber-criminal populations in Canada. This research may contribute toward the enhancement of prevention and suppression strategies, as well as the development of an empirical means for evaluating the effectiveness of initiatives, including elements of Canada's *Cyber Crime Strategy*.

1.0 Introduction

How can information be collected, evaluated, and reported on cyber-fraud offences in a more efficient manner? Clearly, the first step is to identify and define exactly what is being measured. The law typically takes a technology neutral stance to offences (i.e. fraud is fraud whatever the method). Defining criminal phenomena is important because it enables all stakeholders, including police, prosecutors, and judges to have a common understanding. A universal definition also facilitates the aggregation of statistics, which can be used to create an accurate picture of current cyber-fraud related threats and developments. First, a general overview and definition of cybercrime are provided, followed by a discussion of cyber-fraud in all of its many manifestations.

1.1 The Definition and Classification of Cybercrime

Internet use exploded over the last decade, growing five-fold from 361 million users in 2000 to nearly 2 billion users around the globe in 2010 (McAfee 2010(a), 4). The way that Canadians do business has also changed. The use of cheques among consumers has declined while the use of credit cards, debit cards and Internet transactions to make purchases, conduct sales, and manage finances has dramatically increased (Canada 2005, 7). As many as 60% of Canadians now bank online, and in the United States (US), as many as eight out of ten households use online banking (Symantec 2010,12). As with other aspects of globalization, the Internet's rapid growth has far outpaced mechanisms of regulatory control, and this has led to the emergence of new criminal opportunities and presented significant challenges for policing across all corners of the globe.

Cybercrimes come in a variety of forms and there is no standard way of categorizing them. The lack of definitional clarity is troublesome and it affects many aspects of prevention and remediation (Gordon and Ford 2006, 13). Cybercrime is more difficult to define than traditional offline crime because a computer or device can be the agent, target or facilitator of the crime, and the crime can take place on the computer alone or in other offline locations (Gordon and Ford 2006, 13). Generally speaking, computer crime refers to the use of a computer to facilitate or carry out a criminal offence (O'Neill 2000, 241).

Cyber-fraud can be defined as any act of dishonesty or deception carried out through the use of the Internet (or computer technologies) that defrauds the public or any person out of property, money, valuable security or service (Smith and Urbas 2001, 1). Internet fraud can occur as a result of the transmitting of misleading or deceitful information online, by failing to honour contractual agreements entered into online, or through the misappropriation of funds transmitted electronically. Important social cues that help us to avoid fraud in the offline world, such as appearance, facial expression, body language, voice, dress and demeanour, do not operate in the case of Internet transactions, in which agreements are reached instantaneously and payments are made between anonymous individuals operating anywhere in the world. This greatly enhances the ability of individuals to disguise their true identities and intentions, which is an important reason why it is comparatively easy to commit fraud using the Internet (rather than offline).

The Council of Europe's *Convention on Cybercrime* of 2001 defines cybercrime in Articles 2-10 in terms of four substantive categories:

(1) offences against the confidentiality, integrity and availability of computer data and systems;
(2) computer-related offences;
(3) content-related offences; and
(4) offences related to the infringement of copyright and other related rights.

Cybercrime can also include massive and coordinated attacks against the critical information infrastructure of a country, such as the cyber-attacks against Estonia in 2007 (Schjolberg 2008, 9). Not only is the number of threats on the rise, the complexity of attacks has increased precipitously over time (Walther 2004, 7).

One of the central differences between cybercrime and traditional crime is that traditional crime typically occurs in one space and has an impact on one set of victims, whereas cybercrime can have a global impact (United Kingdom 2010, 5). Offenders can operate from anywhere in the world, targeting large numbers of people or businesses across international boundaries. This poses an obvious challenge for law enforcement, and those who commit cybercrime often seek to exploit this challenge, simultaneously undertaking their activities in one country against individuals in many different jurisdictions. Their activities are deliberately targeted in or through jurisdictions where regulation is known to be weak, or where investigative cooperation is known to be poor (United Kingdom 2010, 5). This allows for the minimization of the risk that their activities will be discovered, traced, or result in punishment.

Given the breadth of cybercrime activity and the vast pool of potential victims, it is difficult to arrive at an accurate estimation of the number of cybercrime incidents per year. It is clear that the US had the most overall malicious activity worldwide in 2009, and was the top country of attack origin in 2009, accounting for 23% of worldwide activity (Symantec 2010, 16).[1] However, Symantec reports that malicious activity continues to be pushed to developing countries and in 2009 this trend became more pronounced (Symantec 2010, 7). For the first time since Symantec began examining malicious activity by country in 2006, a country other than the US, China or Germany ranked in the top three.[2] The primary reason is that information security and related laws and policies are less well-developed in emerging economies, providing an environment in which criminal activities can be carried out with less of a risk of detection and apprehension (Smith and Urbas 2001, 2). It is noteworthy that Canada did not rank within the top ten countries for overall malicious activity observed by Symantec in either 2008 or 2009, suggesting that Canada has not become a safe-haven for cybercrime offenders, despite that it has been comparatively slow to enact laws to address the problem.[3]

---

[1] This is a slight decrease from 25% in 2008.
[2] In both 2008 and 2009, the United States ranked number one for attack origin, malicious code, phishing hosts and bots and China ranked number two for attack origin. In 2009, Brazil ranked number three for malicious activity, with Germany ranking fourth (after ranking third in 2008). Symantec reports the top malicious activity by country for 2009 as: the United States (19%); China (8%); Brazil (6%); Germany (5%); India (4%); the United Kingdom (3%); Russia (3%); Poland (3%); Italy (3%); and Spain (3%).
[3] For example, Canada was the last of the G-8 countries to enact anti-spam legislation.

1.3 Defining 'the Victims' of Cyber-Fraud

While individuals (i.e. the general public) are the primary victims of most fraud insofar as they typically bear the financial costs through higher insurance premiums, credit card fees, interest rates, and so on, other victims also exist. A distinction can be made between *primary victims*, including individuals and businesses or public bodies, who initially suffer the harms of fraud, and *secondary victims*, or those who ultimately pay for the economic losses associated with the crime (Levi and Burrows 2008, 304). These include financial institutions, insurance companies, and others who, by contract or regulation, agree to reimburse some or all of the costs to primary victims. It must be stressed that some cyber-frauds are confined to a single class of victims, whereas others overlap, depending on the circumstances of the case (Levi and Burrows 2008, 304). For example, in the case of payment card frauds, victims can include the individual cardholder, the issuer, and the merchant.

The primary purposes of this discussion paper are to assess the potential for using innovative methodologies to estimate the scope of cyber-fraud, as well as existing data sources and gaps, and to suggest novel sources of data that might help provide a more accurate picture of the degree of cyber-fraud in Canada. Thus, it is important to consider the various costs of fraud to different victims, including:

- direct losses suffered by victims as a result of fraud (i.e. the actual amount defrauded);
- costs to the victim(s) of preventing fraud before the event (i.e. both public and private sector entities take certain defensive measures to safeguard against fraud, such as shredding documents or employing IT security measures); and
- costs of responding to fraud after the event (i.e. costs to the criminal justice system, including police, prosecutors and court services, as well as, in the case of organizations, internal private investigations, increased security measures and consumer notification) (Levi and Burrows 2008, 305).

Other indirect losses, which are more difficult to quantify, can result from the reduction in the use of online banking services (assuming that this is more cost-effective for the victim bank) or harm to the defrauded organization's reputation in the marketplace (assuming that this leads customers and other firms to avoid doing business with them). Ultimately, the question of which group or entity shoulders the cost of cyber-fraud is complex and presents a challenge to aggregating the costs of fraud to the Canadian economy (this issue is discussed in detail below).

1.4 The Most Common Types of Cyber-Fraud

Fraud involves purposefully obtaining the property of another through deception, and its popularity as a crime of opportunity is growing. This is largely due to the fundamental shift in the methods by which many forms of property are owned and stored, owing to rapid developments in technology, communications and globalization (Albanese 2005, 7). For example, in Canadian society, credit and debit card transactions are overtaking cash transactions in value, and the rise and growth of the Internet, which facilitates wireless transactions, has made theft, as well as the conversion of stolen property into cash, relatively effortless (Albanese 2005, 7).

Today, identity-related offences are the most common form of consumer fraud. Other examples of Internet fraud include advance fee scams, such as Nigerian scams, lottery scams and inheritance frauds, online auction frauds, and other identity-related and payment card frauds. Internet fraud has been facilitated by obtaining credit card numbers from various online services, which can then be used to fraudulently pay for goods and services ordered online. Included below are examples of some of the most current and pervasive fraud scams on the Internet.

Scareware

Misleading pop-ups suggest that a user's computer is infected with a virus, and prompt them to purchase fake antivirus software to fix the problem. When the victim agrees to the purchase, they provide credit card details to the persons behind the scam. Scareware remains one of the most common Internet threats because it manipulates the psychology of victims (McAfee 2010(a), 7). By playing to Internet users' fear that their computers and their information is at risk, individuals have been able to gain access to users' machines, directly defrauding victims of millions of dollars. In 2009, Symantec observed a dramatic increase in scareware threats in the first six months of the year compared to the last six months of 2008; they further identified 250 variants of scareware being circulated on the Internet (Symantec 2009).

Phishing Scams

Phishing is one of the most prevalent Internet threats today. Recently, attacks have become more advanced in their technical sophistication, by making use of well-known vulnerabilities in popular Web browsers, including Internet Explorer, to install malicious software that collects sensitive information about the victim. Phishing attempts come in a variety of forms, such as through spam emails, or instant messages, and fake requests on social networking sites, often with a link to a realistic but phony Website designed to steal the victim's password, credit card number, or bank account numbers by mimicking the look and feel of a legitimate online banking Website. As discussed below, phishing has been greatly facilitated by the abundance of phishing software kits with easy-to-use point-and-click interfaces being sold inexpensively in the online underground economy. One of the reasons why phishing is so successful is that ordinary consumers are easily fooled by good phishing Websites (Dhamija et al. 2006).[4]

In 2009, Symantec detected 59,526 phishing hosts, which is an increase of 7% since 2008 when it detected 55,389 phishing hosts (Symantec 2010, 18). In 2009, 36% of all phishing URLs identified by Symantec were found to be located in the US (Symantec 2010, 18). Sixty percent of respondents to a survey of Canadians conducted by VISA Inc. in 2005 reported that they would likely provide personal information in response to legitimate-sounding emails, and 4% indicated that they had been phishing victims (Stroik and Huang 2009, 193).

[4] A study by Dhamija et al. demonstrated that good phishing websites fooled 90% of users and that existing anti-phishing browsing cues were ineffective. They also reported that 23% of users do not look at the address bar, status bar, or security indicators and that the average user makes mistakes 40% of the time in identifying phishing websites.

Online Auction Fraud

In an online auction, sellers can hide their identities, which provides sellers a significant opportunity to cheat buyers (Lee et al. 2010, 2991). As noted, the anonymity of the Internet increases the likelihood of opportunistic behaviours on the part of sellers and, in turn, buyers have a great deal of difficulty in trusting sellers and predicting their behaviour (Lee et al. 2010, 2991). Online auction fraud, which occurs both during and after auctions, can involve any one or more of the following scenarios: misrepresentation of items; illegitimate bidding to preserve a low price; intentional fake bidding by the seller to drive the price up; adding hidden charges to an item, such as shipping and handling charges; non-delivery of items; offering black market goods; and fraudulent online credit card transactions (Lee et al. 2010, 2992). Another common complaint is false payment to the seller, including the use of stolen or forged cheques, or through the use of accounts with insufficient funds to cover the payment.

Phony Website Fraud

The process of buying goods and services directly online, without a bid, is also subject to fraud. In recent years, individuals have become increasingly sophisticated at creating fraudulent Websites and consumer products that look real. From fake pharmaceuticals to software products, individuals are always looking for new ways to trick people into entering their credit card data or other personal information.

Online Dating Fraud

The typical online dating fraud begins with the scammer posting an attractive photo on an online dating site (often stolen from a model or minor celebrity). The scammer sends out messages to other members on the site expressing interest. The next step is to engage in a one-on-one conversation with the potential victim, usually through email or instant message. The offender creates a personal relationship in order to ask for cash, merchandise or other favours. Some scammers correspond with their victims for weeks or months, planning, scheming and building trust with gullible individuals they have never met. Victims are enticed by stories that are typically emotionally-laden, financially promising or which have religious overtones. Of course, the scammer only continues to lure the victim and play along until credit card information, bank account details, or actual money can be extracted from the target (Longe et al. 2009, 128).

Nigerian/419 Fraud

The term ‘419’ was coined from s.419 of the Nigerian *Criminal Code* (Chawki 2009). This scam, which is also known as ‘advance fee fraud,’ began with offenders, frequently working from Nigeria, targeting victims across the globe, usually with letters sent through the postal mail. Before long, fraudsters in other jurisdictions, including other African countries, the US, Canada, and Great Britain, began using the Internet to perpetrate this scam. It is commonly known as ‘advance fee fraud’ because it requires the victim to pay the scammer in advance with the promise of obtaining a highly lucrative reward later on (King and Thomas 2009, 207).

The scam usually consists of a spam message from a foreigner who needs help moving millions of dollars out of his/her homeland and offers the recipient a percentage of the funds to assist in the transfer. The offender also asks the victim for a variety of fees up front in order to secure the deal. Typically, the scam is carried out as part of a lengthy interaction with the victim in which the target becomes increasingly drawn into the plot and conned by the scammer's ability to establish sympathy, rapport and trust without ever meeting in person (King and Thomas 2009, 210). The scale of these frauds has increased considerably in recent years and created a worldwide problem for law enforcement. As with all types of cyber-fraud, the complaints to authorities only represent a small fraction of victims. The Canadian Anti-Fraud Centre reported that it received 167 complaints of advance fee fraud from January to September 2004, with losses to victims of approximately $4.2 million (Chawki 2009, 6).

Securities and Investment Fraud

The Internet is now regularly being used for trading in securities and many instances of fraudulent conduct involving the stock market have occurred around the world. Prominent examples include using the stock market to attract investors, or to manipulate markets, which is also known as a 'pump-and-dump' scheme. A pump-and-dump scheme is commonly used to manipulate low-priced (penny) stocks usually from worthless and/or unattractive companies (Paget 2009, 12). After purchasing a large number of shares at a low price, bulk email programs allow rogue stock promoters to send enthusiastic messages to thousands of Internet users. One or two days later, after an artificial rise in the stock price, the scammer sells his or her shares and realizes a quick profit while naïve and greedy investors lose out. The proliferation of online day traders contributes to the volatility of share prices, particularly in those stocks which are thinly traded. This opens up new opportunities for offenders to manipulate share prices, either individually or in conjunction with others. In Canada, the most commonly observed securities frauds are illegal market manipulation, fraudulent high-yield investment schemes, illicit offshore investments, and ponzi (pyramid) schemes (CISC 2010).

Canada's Criminal Intelligence Service reports that securities fraud is becoming increasingly sophisticated and that during the past several years law enforcement agencies have observed cyber-frauds that combine elements from many schemes and involve numerous domestic and offshore facilitators (CISC 2010). The size and complexity of these schemes help to conceal criminal activity and generate substantial profits, as well as facilitating tax evasion and money laundering. Some social networking sites, like *MySpace* and *Facebook*, as well as online bulletin boards like *Craigslist*, have also been used to issue professional-looking but false press releases and promotional materials anonymously and to recruit accomplices. In addition, fraudsters are increasingly using virtual marketplaces, electronic trading systems and wire transfer services to transfer funds anonymously to other jurisdictions. Black-market carding websites are also used to buy and sell stolen account information, and to advertise and trade illicit services.

The CSA Investor Index of 2009 reported that just under four-in-ten (38%) Canadians believed that they were approached with a possible fraudulent investment, a level consistent with findings from 2006 and 2007 (Ipsos Reid 2009, 63). Among those who believed that they were approached, one-in-ten (11%) acknowledged that they invested money in what turned out to be a fraudulent investment. As a percentage of the total population of Canada, this means that 4% of

Canadians have been fraud victims, the same incidence as reported in 2006 and 2007 (Ipsos Reid 2009, 6). Canadians are most commonly targeted for investment fraud through email (33%), by a stranger on the telephone (28%), or through a friend, family member or coworker (18%) (Ipsos Reid 2009, 5). The amount invested in fraudulent investments has also apparently increased. In 2009, 38% invested in $5,000 or more, compare to 32% in 2006. The average amount invested is $7,634 across Canada. Most money is never returned to victims.

One in-four Canadians (26%) say that they reported the attempt to authorities, compared to 17% in 2007, and 14% in 2006 (Ipsos Reid 2009, 5). Yet, among Canadians thinking that it is important to report suspicions that someone has approached them with an investment fraud has declined since 2006.[5] Those who did not report the attempt most likely did not do so because it was email spam (16%), they did not think that reporting it would do anything/make a difference (12%), they were not sure it was fraud (12%), they felt they had nothing concrete to report (11%), and/or they preferred to just ignore it (11%) (Ipsos Reid 2009, 5).

Identity-Related Fraud

One of the most common strategies to perpetrate fraud is the creation of false documents for misrepresenting identity. Once a fraudulent identity has been convincingly established, it is then possible to steal money or otherwise act illegally and evade investigation and prosecution. The Internet facilitates this sort of fraudulent activity by making it easy to manipulate email and Internet addresses, and to obscure the source of a message through the use of technological tools, such as anonymizers, anonymous remailers and the like.

Credit card fraud is the most common incident of identity-related fraud (Berg 2009, 227). For example, the UK Government reported that loses from credit card fraud where the consumer's card was used without them present were 328 million pounds in 2008 (an increase of 13% from the previous year) (United Kingdom 2010, 5). In this scenario, the offender uses the victim's identity in order to apply for and obtain new credit cards or fraudulently uses an existing card belonging to the victim. Other examples of identity-related fraud include using the stolen identity to obtain phone services, or another utility; opening bank accounts using the victim's information or writing cheques against the victim's account; obtaining employment in the victim's name; obtaining a driver's license or other government-issued identification in the victim's name; filing fraudulent tax returns; or taking out a loan in the victim's name.

Credit Card Fraud

From early on in the history of e-commerce, online fraudsters targeted credit cards (Wall 2010(a), 70). Internet users have reported being concerned about the collection and use of the personal information they supply while shopping online (Sheehan and Hoy 2000, 62); however, they are

[5] Eight-in-ten (78%) Canadians agree that it is important to report suspicions that someone has approached them with an investment fraud (of which 40% agree strongly, compared to 53% in 2006, and 38% agree somewhat, compared to 33% in 2006).

frequently willing to trade-off their privacy concerns in return for benefits such as convenience (Chellappa and Sin 2005, 181). This trend is problematic because goods and services can easily be obtained using active cards that have been obtained through illicit means. Also, they can be obtained using counterfeit credit cards created from stolen information, such as through the online underground economy, discussed below. Credit cards can also be cloned using illicit card readers (known as 'skimming') during an otherwise legitimate transaction, or from discarded credit card receipts (Wall 2010(a), 70).

The online credit card fraud (or 'carding') marketplace has evolved significantly in recent years. As discussed below, there are large, heavily moderated forums devoted to enabling offenders to buy and sell stolen information and products, share tips and techniques, and post cybercrime related news stories (Howard 2009, 28). Several high-profile law enforcement operations (most notably 'Operation Firewall' in 2004) caused many once prominent carding operations to move underground; hence, much of the current online communication about carding is conducted through secure channels, such as Internet Relay Chat (IRC) rooms, messaging services and email (Howard 2009, 26). In 2009, combined losses due to payment card fraud in Canada decreased slightly from $512.2 million in 2008 to $500.7 million in 2009 (CISC 2010, 29). At the same time, losses due to debit card fraud increased by 36% from $104.5 million in 2008 to $142.3 million in 2009 (CISC 2010, 29).

Insider Fraud

Internal employees can use the Internet to anonymously gain access to data that is not related to their jobs and misuse it for personal gain (Campbell 2009). Opportunities have arisen for employees of both public and private sector entities to commit a variety of online frauds, such as manipulating electronic claims processing systems, compromising digital signature keys, or altering/diverting electronic fund transfers away from legitimate recipients (Smith and Urbas 2001, 54). Rogue insiders can also gain electronic access to the records of customers and other employees and use those records to fraudulent ends. These malicious acts are commonly perpetrated by current employees and contractors as well as disgruntled former employees who have been dismissed, laid off, or who have resigned.

It is also significant that 'well-meaning' and/or negligent insiders pose an additional threat by disclosing data that can be used by malicious outsiders against the organization (Wall 2010(b), 3). Indeed, in 2009, in the US, 40% of data breaches, and 46% in the UK, were estimated to result from insider negligence (Wall 2010(b), 3). In some cases, insiders use very simple passwords, or may use one password for all of the secure sites they access. Alternatively, they might write down passwords on post-it notes attached to computer screens or circulate them to colleagues to check their email messages for them (e.g. if they are away on vacation) (Wall 2010(b), 9). Others knowingly take risks to bypass security processes in order to become more efficient at work (Wall 2010(b), 9). In other cases, employees can be duped by malicious outsiders into sharing sensitive information or giving access to systems, through 'social engineering' scams because they genuinely believe that they are being helpful and acting in good faith (Wall 2010(b), 10).

2.0 The Prevalence and Cost of Cyber-Fraud

Is cyber-fraud, in all of its manifestations, a serious problem in Canada? How does it compare to the frequency and costs of other kinds of crime? While there are many accounts of cyber-fraud documented in the electronic and print media, the frequency with which cyber-fraud occurs and the losses that result are extremely difficult to ascertain with precision. Canada does not have a uniform method of collecting data on cyber-fraud.

As with other kinds of fraud, Internet fraud is rarely reported to law enforcement authorities. This makes it extremely difficult to quantify the scale and scope of the problem. The shortage of valid and reliable statistics has severely hampered our understanding of the nature, prevalence and impact of cyber-fraud, as well as the ability of law enforcement to respond to it. The principal sources of information concerning fraud are business victimization surveys, and consumer reporting centres, as well anecdotal accounts of successful criminal prosecutions that are reported through the media. The incidents of Internet cyber-fraud that are disclosed to the public represent a small proportion of the total number of incidents that occur, which means that there is a need for more systematic data to be collected on the nature and extent of Internet fraud in Canada.

There are a variety of important reasons why businesses elect not to report fraud to the police. They may be reluctant due to the fear that the incident was too minor or that it will be impossible to recover losses successfully through legal channels and that the time and resources needed to report an incident to the authorities and to assist in its prosecution do not justify the potential return on this investment (Smith and Urbas 2001, 41). In such cases, they may decide to rely on other means, such as using internal or private investigators and/or reporting the incident to entity other than law enforcement (e.g. PhoneBusters, FINTRAC, or the Better Business Bureau) (Taylor-Butts and Perreault 2008, 12). The other major disincentive for organizations to report is the disinclination to publicize the victimization because of a fear of losing business or harming their commercial reputation in the marketplace (Smith and Urbas 2001, 42). Governments, for their part, are reticent to disclose IT security breaches due to the risks of alienating voters and losing trust in the public service.

There is clearly a need for more systematic data to be collected about the nature and amount of cyber-fraud in Canada and for extensive analysis of the problem. It is also significant that, in the limited cases where research does exist, there are numerous data-related and methodological problems (White and Fisher 2008, 13). For example, there is no consistent definition or use of the terms ‘identity theft,’ ‘fraud,’ and ‘cyber-fraud’ across agencies or organizations. This means that when data are available, they may not be comparable. Data is also affected by a number of agency-specific variables, including budgets, staffing, resources, awareness of the problem and national response. There is also the difficulty of generating a random sample of victims of cyber-fraud or identity theft because those who do contact law enforcement or an agency are not necessarily representative of all victims. Thus, studies that identify victims based on prior contact with an agency, law enforcement, or even by survey, are not likely to capture all fraud/identity theft victims and offences.

Indeed, there are few reliable statistics on the prevalence of fraud, and there is no precise way of assessing how much of this type of activity occurs, largely because a significant proportion of

incidents will not be reported, identified or even detected by victims. Some indication of the prevalence of cyber-fraud is available through surveys of industry groups and households. Generally speaking, though, there are few centralized sources of data within the private sector, and the information that does exist is not complete, nor is it comparable across businesses (Canada 2005, 12). Apart from victims being difficult to identify and reach, information about fraud is derived from a variety of sources, many of which suffer from methodological shortcomings (Levi et al. 2007, 8).

Official statistics do not always identify the specific means by which cyber-fraud is perpetrated, making it difficult to establish the scope and scale of the problem. In the absence of more reliable and accurate information, the precise nature and extent of the problem cannot be documented. The Uniform Crime Reporting Survey was developed by Statistics Canada with the cooperation of the Canadian Association of Chiefs of Police (Canada 2005, 35). The survey, which became operational in 1962, collects crime and traffic statistics reported by all police services in Canada with respect to crime that has been substantiated through police investigation (Canada 2005, 35). In other words, official statistics about fraud in Canada, collected through the Uniform Crime Reporting Survey only reflect incidents of fraud that were reported to the police (Taylor-Butts and Perreault 2008, 5). The data element "type of fraud" is used for recording any fraud that involves the unauthorized use of a computer or use of a computer for illegal means, including hacking, illegal use of user ID, or personal password (Kowalski 2002, 17). The addition of the data element "cyber-crime," which was added to the UCR2 survey in 2005, allows police to indicate whether a computer or the Internet was used as a tool to commit fraud. However, the Uniform Crime Reporting Survey does not allow the data to be further broken down to identify the specific kinds of fraud that are being committed through a computer or the Internet.

In addition, the Canadian Bankers Association (CBA) releases reports each year about credit card fraud in Canada (CBA, 2011). The CBA recently reported that, for the year ending December 2009, 45,103 credit cards were reported stolen, which resulted in a CAD$27,208,823 loss to Canadians.[6] The average loss per card was only $693.26. There were 2,442 fraudulent credit card applications in Canada in 2009, according to the CBA, and this resulted in a loss of CAD$4,707,088, with an average loss of CAD$1,927.55 per account. There were reportedly 294,549 fraudulent e-commerce, telephone and mail credit card purchases, amounting in a CAD$140,443,893 loss in 2009, with an average loss per account of CAD$476.81.

While many global or North American surveys likely include Canadian respondents, only a small number of studies have explicitly focused on Canada. In 2007, the CATAAlliance conducted a survey of 322 Canadian IT security professionals to identify significant IT security challenges (Wennekes 2008). The responses show that most Canadian IT security professionals rely on their personal networks of IT experts for guidance. The responses also highlight a lack of current best practices as an important challenge facing their organizations. Best practices are typically formed out of collective wisdom and then shared with others (Wennekes 2008). This sharing is vital to

[6] This includes Amex, MasterCard and Visa only. Note this is distinguished from lost cards (22,304 Canadians reported their cards lost).

establishing a common body of knowledge about the optimum practices to maintain information security.

The study indicated that Canadian IT security professionals consider colleagues and personal networks to be their primary sources of IT security information (Wennekes 2008). It is significant that these individuals reported feeling highly comfortable with using personal networks. Among personal networks there is less chance of appearing uninformed or technically challenged, and those who are part of a personal network are clearly seen as credible sources of information. These findings substantiate the research evidenced by Canadian IT security professionals, as discussed below in subsection 9.2. These findings suggest that new initiatives, such as creating an online database of best practices which IT security professional members can add to and view, and/or developing an online community (e.g. to send out advice and tips) and holding best practice information sessions/conferences within specific industry sectors, could be instrumental to proactively responding to cyber-fraud threats, as well as gathering reliable information about current threats and vulnerabilities.

Another source of information on cyber-fraud is Statistics Canada's *Survey of Fraud Against Businesses* in 2008, which focused on 4,330 Canadian businesses in the retail, banking and insurance industries (Taylor-Butts and Perreault 2008). Overall, 57% of retailers, 45% of insurance agencies, and 84% of the banking institutions in the country that provided information had experienced fraud in the previous 12-month period. In the retail sector, the most common types of fraud committed were return fraud (81.2%), followed by the fraudulent uses of credit cards (32.1%), counterfeit money (15.2%), and the fraudulent use of cheques (15.0%). In the banking sector, the most common types of fraud included the fraudulent use of debit cards (49.8%), the fraudulent use of cheques (29.1%), worthless deposits (9.9%), and the use of counterfeit money (6.2%). With respect to the health and property insurance industries, the most common types of fraud were insurance claim fraud (77%), advance fee schemes (est. 21.7%), and false billing (est. 17.3%) (Taylor-Butts and Perreault 2008). Interestingly, 7 in 10 individual retail establishments and about half (52%) of banking establishments that experienced fraud or were victims of an attempted fraud in the previous 12 months indicated that these acts were committed in-person by those perpetrating the fraud (Taylor-Butts and Perreault 2008). Regular mail was the most common method used to defraud insurance establishments (32%) and banks reported that the Internet (23%) and email (17%) were the top methods of fraud utilized in acts of fraud they had experienced (Taylor-Butts and Perreault 2008).

The authors found that nearly half of retailers (47%) and insurance establishments (47%) said that in general, they never or only rarely notify law enforcement in cases of fraud (Taylor-Butts and Perreault 2008, 12). Fewer than 1 in 5 retail establishments that had experienced fraud indicated they had reported the activity to either PhoneBusters (i.e. the Canadian Anti-Fraud Call Centre) or to the RCMP's RECOL (Reporting Economic Crime On-Line) (Taylor-Butts and Perreault 2008, 12). Official statistics are likely to under-estimate the number of fraudulent criminal activities committed against these types of businesses in Canada.

In addition, the Royal Canadian Mounted Police (RCMP) and the Ontario Provincial Police (OPP) currently operate two separate initiatives for the centralized reporting of fraud. The RCMP operates the Web-based Reporting Economic Crime On-line (RECOL) and the RCMP and OPP

jointly operate PhoneBusters (which has been re-named the Canadian Anti-Fraud Centre) to collect fraud complaints, share evidence with other enforcement agencies about the dollar values lost, the characteristics of victims and the geographic location of incidents, as well as to educate the public about scams. In 2005, these two initiatives standardized the information they collect (i.e. data about economic crimes via phone, Internet, fax and email) yet the two databases have remained separate (Canada 2005, 13).

The 2010 *Annual Statistical Report* by the Canadian Anti-Fraud Centre Criminal Intelligence Analytical Unit reported that there was an increase in mass marketing fraud[7] complaints in Canada from 36,470 complaints in 2008 to 48,837 complaints in 2010 (Canadian Anti-Fraud Centre 2010). Interestingly, the total number of victims and the total reported dollar loss decreased from CAD$59,273,771.99 in 2008 to CAD$53,843,364.58 in 2010. The average age of the Canadians most commonly targeted by mass marking fraud was between 50 and 59 years. In 2010, there were 11,783 Canadian complaints on Canadian-based mass market fraud operations, with 2,752 Canadian victims (Canadian Anti-Fraud Centre 2010). The total loss to Canadian victims was CAD$12,748,068.93 (up from 7,674 complaints and CAD$10,370,441.40 lost in 2009). Ontario was the top province targeted by mass marketing fraud in 2010. The top method of solicitation, based on Canadian complaints, was telephone/facsimile, followed by email/Internet/text message (and these victims reported the highest total reported dollar loss). Based on the total number of complaints, 'Service' was the top reported mass marketing fraud scheme reported by Canadian consumers.[8] The total reported dollar loss on Canadian-based mass-marketing fraud schemes by international victims in 2010 was CAD$8,960,571.96. The total number of Canadian identity fraud complaints and victims also increased in 2010 but the reported dollar loss decreased. Western Union was the top reported payment method used to receive funds from Canadian victims.[9]

In 2008, TELUS and the University of Toronto's Rotman School of Management jointly implemented a study to provide information about the state of IT Security in Canada (Hejazi et al. 2010, 228). Responses from 300 IT and security professionals in Canada allowed them to understand how Canada differs from the US in terms of cyber-threats and vulnerabilities. A follow-up study was conducted in 2009 with 600 Canadian organizations and government agencies. The study findings indicated that respondents reported a much higher number of breaches than in 2008 (11.3 per year in 2009 up from 3 per year in 2008). Further, the study showed that annual losses from breaches increased to CAD$834,149 per organization, up from CAD$423,469 per organization in 2008. In addition, in 2009, Canada caught up to the US in terms of the number of breaches: 14% of Canadian companies reported experiencing financial

[7] Mass marketing fraud includes phishing, charity/donation schemes, sale of merchandise scams, collection agency scams, job offer scams, prize scams, and merchandise and service scams (which are undefined).
[8] Note that 'sale of merchandise by complainant' is the top reported international mass marketing fraud scheme and 'Prize' is the top reported Canadian-based mass marketing fraud scheme reported by American consumers.
[9] It must be kept in mind, though, that this information was not representative of fraud in Canada because individuals and businesses that do choose to report to police may report to their local police service rather than these centralized initiatives (Canada 2005, 14).

fraud in 2009 compared to 12% of American companies in 2008.[10] In 2009, the number of reported breaches in Canada increased: unauthorized access to information by employees increased by 112% from 2008, and financial fraud increased by 75%. According to the 2009 research, the financial crisis adversely impacted IT Security programs, with respondents reporting an average IT Security budget decrease of 10%.

A subsequent follow-up study was conducted in 2010 with 523 Canadian organizations and government agencies (Begin 2010(b)). The authors reported that in 2010, IT security budgets remained below their 2008 levels. The number of reported breaches grew by 29% over 2009, and the majority of the increase affected government entities. In 2010, Government entities identified by the research reported experiencing on average 22.4 breaches, a 74% increase from the 13.4 breaches reported in 2009. Another trend identified by the research was that while the abuse of wireless networks, denial of service attacks, and Website defacements declined, there was an increase in social engineering attacks, "that exploit user trust in relationships," such as phishing scams. Botnets, which are often the distribution mechanism for these types of attacks, were also said to be on the rise. Finally, identity theft and the theft of confidential customer information were also reported to be on the rise.

A number of studies conducted in other jurisdictions also help to highlight the costs of cyber-fraud over a specific time period. However, data collected outside Canada also have a number of problems in terms of its reliability and accuracy in measuring the cost of cyber-fraud. The total dollar loss from all cases of Internet fraud and scams referred to US law enforcement agencies in 2008 was USD$264.6 million – an increase of 10% from the previous year – representing a 32% increase from USD$68 million in 2004 (Wagner 2009). The Consumer Sentinel in the US reported that it received 370,012 fraud complaints in 2008, with 193,817 (52%) related to email and 40,596 (11%) related to the Internet (Website/other) (Paget 2009, 4). Consumers reported fraud losses of over USD$1.2 billion that year; the median monetary loss was USD$349. As many as 64% of these complaints involved the Internet as the method of solicitation, with 49% related to email and 15% related to the Web.

According to the US Internet Crime Complaint Centre, the total loss from fraud on the Internet reported to them was USD$560 million in 2009, with the most significant loss coming from the non-delivery of goods (United Kingdom 2010, 13). In 2008, the Centre reported that Americans filed 33.1% more complaints than in 2007, and the total amount of money stolen online reached a historic record (Paget 2009, 4). In 2008, the Claims Centre registered almost 275,000 complaints, representing a loss of USD$265 million, or 10.6% more than in 2007 (Paget 2009, 4). Half of all cases involved a monetary loss of less than USD$1,000 and one-third (33.7%) of those filing complaints reported losses between USD$1,000 and USD$5,000 (Paget 2009, 4). Only 15% of complainants indicated a loss more than USD$5,000. Auction fraud and the failure to deliver purchases were the most widely reported complaints to that centre.

[10] Note, also that one of the weaknesses of the study was that it compared security breach statistics in Canada from 2009 to those reported by the US's Computer Security Institute's annual computer crime survey in 2008. Had the researchers compared statistics from both countries in the year 2009, they may have concluded that Canada's breach record was not worse than that of the US.

The Australian Bureau of Statistics' (2008) National Personal Fraud Survey, conducted throughout Australia from July to December 2007 estimated that nearly A$1 billion was lost as a result of personal fraud and that nearly half a million Australians experienced a form of identity fraud during that time period (Smith 2008, 379). The UK Government has reported that losses from credit card fraud, where the consumer's card was used without them present were GBP$328 million in 2008 – an increase of 13% from the previous year (United Kingdom 2010, 5). In 2010, the UK's Home Office Identity Fraud Steering Committee reported that the cost to the UK economy from identity fraud was at least GBP$1.2 billion and accounted for a criminal cash flow of some GBP$10 million per day (United Kingdom 2010, 13). Online banking fraud losses in the UK increased 185% from 2007 to 2008, and phishing incidents increased 186% during that same period.

It is clear that there has not been extensive effort, in Canada, the US, Australia, or the UK, to measure the nature and extent of cyber-fraud. There has also been little attempt to understand the broader social and economic costs of cyber-fraud, such as anticipatory costs. Nor has there been a unified endeavor to clarify the meaning of this deceptively simple term, which encompasses a wide and disperse set of behaviours, victim characteristics, delays in awareness/notification and reporting, and investigative costs. Also, the different objectives behind the various data collection exercises have led to vast differences in methodological strategies. This has understandably hampered knowledge.

These studies represent the publicly available, methodologically sound sources which provide information about the scope and scale of cyber-fraud. While they are able to provide some current data on fraud and enable us to make some conclusions about the nature of cyber-fraud, they have limitations. The data are not routinely collected annually in each survey – for example, while the *Rotman-Telus Joint Study on Canadian IT Security Practices* was conducted three years in a row, from 2008 to 2010, the *Survey of Fraud Against Businesses* was only commissioned in 2008. The surveys used different methods to assess the frequency and costs of fraud and they also covered diverse business sectors and types or sub-categories of fraud. They were further derived from various organizations, with differing employee size, and not the economy as a whole. There has also been little effort documented in the literature to determine where frauds originated, which is particularly important in the case of cyber-fraud, which is often committed trans-nationally.

In addition, many of these sources were drawn from surveys based on opinions of fraud, which are not as robust as administrative statistics when trying to measure the costs of fraud. For example, surveys of victims often ask 'have you been a victim or this or that fraud?'; this question fails to acknowledge that these types of frauds are confusing and complex, even for seasoned anti-fraud professionals, who may also find the precise meaning of certain kinds of conduct labeled as fraud to be unclear (Levi and Burrows 2008, 304). Data on certain types of fraud are also not available, largely because studies have not been carried out on them, or because information about them is either unknown or confidential, and it is therefore unclear whether these types of fraud (e.g. online dating fraud or identity-theft related fraud) are only of limited concern or are completely underestimated. In addition, data tend to be collected only about fraud losses, and little is known about anticipatory or preventative losses.

3.0 Cyber-Fraud, Organized Crime and the Online Underground Economy

From a policy and law enforcement perspective, it is critical to understand whether or not the frauds being committed in Canada are being committed by individuals within or outside Canadian borders (Canada 2005, 21). Thus, the involvement of organized criminal groups in fraud is an important issue, regardless of whether they are simply trying to make fast and easy money or are using proceeds from fraud to finance other criminal activities. Current discourse on the link between computer technologies and organized crime continues to be fraught with rumour and exaggeration; however, in the context of a globally pervasive Internet, many kinds of organizations, both legal and illegal, are increasingly dependent on the Internet for their functioning and success (Grabosky 2006, 187). It is clear that cyberspace provides many kinds of criminal actors with a safe haven that also enhances their organizational and operational capabilities.

For the purposes of this section, a criminal organization is an association or group of at least three people that devote the majority of their efforts to committing illegal activity for the primary purpose of material benefit (Brenner 2002, 7). This definition is derived from section 467.1 of the Canadian *Criminal Code,* which defines a criminal organization as

> a group, however organized that (a) is composed of three or more persons in or outside Canada; and (b) has as one of its main purposes or activities the facilitation of one or more serious offences that, if committed, would likely result in the direct or indirect receipt of a material benefit, including a financial benefit by the group or by any of the persons who constitute the group.

Criminal organizations are structurally diverse and must be identified along a continuum (Morselli 2010). At one end, are time-honoured organized crime groups, such as the American Mafia, which have complex organizational structures, emphasizing a hierarchical division of labour, as well as close ethnic/familial ties. They tend to focus their activities on local endeavors, such as drug dealing, money laundering, loan sharking, illicit gambling and prostitution (Brenner 2002, 7). At the other extreme, there are many examples of criminal networks that are loosely structured and involve many small networks comprised of multiple actors (Morselli 2010). There is no incongruity between short-term criminal networks, with shifting ties and loyalties, and more formal criminal organizations. Indeed, both kinds of organizational structures have existed for many years and they are sometimes interconnected (Morselli 2010, 16).

New criminal networks that are relatively small, global, ethnically/culturally diverse, loosely structured, transitory and goal-specific have formed within cyberspace (Brenner 2002, 45). They typically operate as partnerships between independent actors (e.g. developers, traders or brokers) (Morselli, et al., 2002, 22), mainly due to the Internet's unique structure as a network of networks, which is diverse, fluid and highly generative (Brenner 2002, 39). Online criminal networks tend to be characterized by collaboration and have little organization. For example, small, informal hacker groups have developed, such as cnxhacker and milw0rm, which are a form of cyber-gang that tend to operate laterally (Brenner 2002, 26).

Many such groups have adapted to technological change and used computer technologies to facilitate their offline criminal activities, such as drug trafficking and money laundering. Online auctions provide a means to move money through seemingly legitimate purchases, and as e-money and electronic banking become more prevalent, opportunities to hide the movement of the proceeds of crime in an increasing array of illegal transactions are likely to increase. In other cases, organized criminals have used the Internet to develop new crimes and expand upon traditional ones.[11] Examples of traditional organized crime groups engaging in technology-enabled crime include the Asian Triads and Japanese Yakuza whose criminal activities have included computer software piracy and credit card forgery/fraud (Choo 2008, 273).

Criminal groups have been able to focus their efforts on publicizing software vulnerabilities they discover, writing malicious code and developing sophisticated new hacking techniques (Choo 2008, 277). They have also been able to increase their attacks exponentially through the growing use of automation and by providing widespread access to their malicious code (UNDOC 2010, 204). Many millions of spam email messages can be sent out by automation within a short time period and customized software tools now enable neophyte attackers to target thousands of potential victims within hours (UNDOC 2010, 204).

In addition, the ability to gain access to a wealth of products, services, and information from other individuals around the world enables offenders to combine efforts to accomplish highly sophisticated attacks which are far more complex than victimizing a single person or entity (UNDOC 2010, 28). Virtual criminal networks are often focused around an online meeting place, either through a Web forum or an Internet Relay Chat (IRC) channel (United Kingdom 2010, 11). IRC is an Internet communications protocol with a number of appealing features: it offers real-time group communications; it is always 'open' and requires little bandwidth; and the software is freely available across all operating systems (Symantec 2008, 5). In contrast to the Web forums, which have maintained a surprisingly indiscrete presence on the Net, IRC channels typically hover below the radar and are far more transitory in nature (Symantec 2008, 9).

There are also a number of large, moderated Web forums devoted to enabling offenders to buy and sell stolen information and products, share tips and techniques, post cybercrime related news stories or just socialize (Howard 2009, 28). These forums tend to have relatively short life spans due to the risk of detection by law enforcement (Howard 2009, 28). Yet, while they are appropriately defined as a loose affiliation of participants, there is a certain degree of collaboration and organization within these groups (Symantec 2008, 8). The various forums have different levels of membership, with some allowing members to immediately post advertisements and interact with other members, while others conduct a peer-review process for potential sellers and restrict member privileges until certain criteria are met (Symantec 2008, 4).

[11] For example, Morselli et al. mention a study by Icduygu and Tokas (2002) that looked at human smuggling in the Middle East and Turkey. The authors found that the traffickers generally had access to the latest communications technology, including mobile phones, and that because of this reliance on modern technology they were able to run their smuggling operations more efficiently, with less chance of detection and apprehension.

This process is understandable given that secrecy is usually a central aspect of any organized crime activity, and the Internet provides a high degree of concealment to those who use it. Faced with the perpetual threat of identification and apprehension, many participants in criminal organizations try to reduce the likelihood of detection by police or betrayal by accomplices by trying to build trust and group solidarity between participants (Morselli 2011, 26). In the case of many online criminal networks, members rarely meet in person and individuals are often known only by their cyber-aliases or nicknames (Morselli 2011, 26). Individual members can connect with other individuals with the requisite technical skills on an as-needed basis, masking their identities and significantly reducing the risk of being caught. Many Web forums are self-policing and have safeguards that can be used as protections, such as to weed out disloyal 'rippers' (i.e. scam artists who prey upon other criminals by ripping them off) (Morselli 2011, 26).

Many online crime groups also have a home base in states with few or no laws directed against cybercrime. This provides an additional layer of protection against law enforcement and enables them to operate with few risks. In Russia, for example, the lack of economic and employment opportunities has forced many highly educated individuals with strong computer programming and technical skills to work in the illicit cyber world (Choo 2008, 275). The Shadowcrew, which had a number of administrators and contacts who resided in Russia, was an international identity theft network which hosted an online forum that shared information about stealing, trading and selling personal information that could be used to commit fraud. It was one of the first groups to obtain notoriety as an active Web forum for online fraud (Symantec 2008, 9) and it reportedly was involved in the trafficking of more than 1.7 million credit cards online (Choo 2008, 277).

The Shadowcrew practiced a form of 'ad-hoc organized crime': they worked remotely without ever needing to meet, and came together for specific purposes (Menn 2010, 173). Some members of the group were in charge of running forums on the Website which discussed strategies for stealing identities, spamming and forging documents, among others (Symantec 2008, 9). These forums were attractive to many new participants, with a variety of skill levels, and enabled neophytes to enter into the trade through the underground economy (Symantec 2008, 9). Other members focused on hacking into the cash register systems of various companies to test whether stolen credit card numbers would be accepted and rating the stolen personal identification documents, which would later be offered for sale on the forums or through an online auction site. Additional members were responsible for the sale of the stolen information, as well as money laundering; and, lastly, a number of members were in charge of gathering credit card numbers and providing instructions on how to obtain and falsify identity documents (Zambo 2007, 557). This is characteristic of how many modern e-crime networks are organizing themselves (Wall 2009, 55). Schemes such as the Shadowcrew's highlight the trans-national nature of cybercrime and the ability of individuals to come together online to provide specialized services and supplies to carry out illicit operations (Symantec 2008, 12).

There were as many as 4,000 registered Shadowcrew members from around the globe whose activities were organized around one Website – www.shadowcrew.com – to deal in credit card wares between August 2002 and October 2004 (Hilley 2006, 10). The group made little effort to hide its illicit purpose; it was open to the public for registration and viewable by anyone, making it easy for law enforcement to monitor their activities (Symantec 2008, 9). The members of the group used spamming and phishing techniques to capture credit card numbers that were used to

purchase goods which were later sent to an address specifically designed for that purpose (Hilley 2006, 10). They also stole passports, bank account numbers, and US social security numbers. Their crimes are estimated to have cost more than USD$4 million (Hilley 2006, 10). In 2005, the group was brought down by 'Operation Firewall,' an eighteen-month undercover investigation by US and international law enforcement agencies (Hilley 2006, 10).[12]

The Russian Business Network (RBN), a Russian-based criminal organization, was also identified by VeriSign as be a service provider of phishing sites and repositories of malicious code in recent years (Choo 2008, 280). It was recognized for creating approximately half of the phishing incidents that occurred worldwide in 2006, and for hosting Websites that were responsible for a significant portion of the world's Internet crime (Symantec 2008, 9). The RBN was an Internet Service Provider (ISP) based out of St. Petersburg that only hosted illegal and malicious items, including fraudulent Websites and malicious code (Menn 2010, 171). For example, Rock Group, an organization specializing in phishing, used its hosting services and was estimated to have made USD$150 million in 2006. In addition, a number of prolific pieces of malicious code (i.e. attack kits or toolkits) were developed and distributed within RBN networks (Symantec 2008, 13).

Almost all of the targets of the RBN were financial institutions, and their customers were primarily based outside of Russia. The lack of Russian targets, as well as the organization's close ties to the Russian government, gave local law enforcement agencies little incentive to take legal action against the RBN, which made investigations by authorities in other jurisdictions difficult (Menn 2010, 171). The RBN was connected to number of other local ISPs, with which they shared IP addresses, service providers, and interconnected registration and contact information. In this manner, the RBN brazenly operated within a network of illicit Russian-based ISPs that facilitated interactions between offenders (Menn 2010, 172). The RBN did not have its own Website and was only accessible to those with connections to the individuals running the network (Symantec 2008, 14).

In 2007, the RBN shifted its operations from Russia to ISPs with Chinese and Taiwanese IP ranges (Menn 2010). At the same time, though, increased media, law enforcement and security industry scrutiny about the amount of criminal activity being facilitated by the RBN led to the deletion of a number of domains controlled by the RBN and their Chinese/Taiwanese operation was also halted. These shut-downs did not lead to sweeping arrests. However, the model of a large-scale and consolidated network of illicit ISPs within a single country has been weakened (Menn 2010). Instead, criminal service providers now typically offer a diffuse arrangement of services rented from legitimate ISPs across several countries, thus decreasing the likelihood that the full scale of their illicit operations will be detected and halted (Menn 2010).

The underground economy has also evolved into an increasingly mature global marketplace where technical skills and data can be purchased to carry out specific attacks. Symantec reports that readily available code kits, or crimeware kits, which are widely available for sale on the

[12] Note that two other Web forums devoted to online fraud, Carderplanet and Darkprofit, were also shut down as a result of this investigation.

underground economy, are making it easy for novice attackers to compromise computers and steal information (Symantec 2010, 11).

A crimeware kit is a toolkit that allows people to customize a piece of malicious code designed to steal data and other personal information (Symantec 2010, 11). The success of these kits as a means of cyber-attack was demonstrated in 2009 when the top five phishing kits observed by Symantec were responsible for a combined average of 23% of all observed phishing attacks for the year (Symantec 2010, 18). The lowering of barriers for neophytes to enter into the cybercrime realm has been evident in the increase in malicious code threats that use remote access capabilities to steal confidential information (Symantec 2010, 18). For example, the well-known Mariposa botnet (a botnet or robot network is a term commonly associated with malicious software), which infected more than 15 million computers around the world, was perpetrated by attackers with limited computer skills who downloaded the software program from the Internet for less than a thousand dollars (Deloitte 2010(b)). This indicates that the online underground economy has flourished while the mainstream economy has only just begun to recover from the global financial crisis (Symantec 2010, 15).

Credit card information, which is typically sold in bulk packages, was the most commonly advertised item for sale on the underground economy servers known to Symantec in 2009 and was advertised for USD$0.85 to USD$30.00 per credit card number (Symantec 2010, 18). The US had the most credit cards advertised on underground economy servers of any country, accounting for 67% of the total (Symantec 2010, 18).[13] As a general rule, cards from European and Asian countries are more expensive than those from the US or Canada (Panda 2010, 18). Details from cards issued in the US can cost as little as USD$2 for basic information and up to USD$40 for Gold, Platinum and Business with complete information (Panda 2010, 18).

Stolen credit card information must still be converted into hard cash, and criminals are always looking for innovative ways to achieve this end (Panda 2010, 7). The process by which stolen credentials are converted into valid currency or merchandise is known as 'cashing out' (Menn 2010, 25). Typically, cyber-criminals employ users as unwitting accomplices or 'money mules' to assist them with the cash out process. The name 'money mule' comes from the transport method that smugglers used to move illegal goods; today it describes individuals recruited over the Internet who serve as intermediaries for recovering cash in funds that were illegally acquired through phishing, keystroke logging and other online scams (Paget 2009, 10). The mule provides his or her bank account to the criminals, who then use it to process stolen funds or purchase goods for later resale (Menn 2010, 35). Mules typically receive direct deposit payments to their personal account within the same country as the victim from whom the money is stolen and then withdraw the cash and make an overseas wire transfer to an account specified by the criminal (collecting a certain percentage of the transfer or a base salary).

To recruit mules, offenders post false job advertisements, offering a high commission, often spamming ads for positions through email or legitimate career Websites such as *Monster.com* (Menn 2010, 35). For each transaction, the mule gets a percentage of the committed amount,

[13] This remained unchanged from 2008.

forwarding the balance through an anonymous money transfer service (such as a wire transfer service like Western Union). Mules are often individuals who are looking to make easy money, and this job has become particularly popular in the wake of the global financial recession. Mules can be made victims themselves; they frequently do not know what they are doing and simply see the transaction as an easy way to make money (Panda 2010, 13).

Social networking and constant online communication, as well as the abundance of communication devices, networks and individual users, have also led to new risks and illicit opportunities. With the advent of social networking sites, like *Facebook* and *Twitter*, individuals have gained access to a wealth of useful information and potential targets. With users posting everything from where they live to what they are doing at any given moment, it is easy for strangers to gain access to personal information by way of social engineering, the art of conning or manipulating people into disclosing personal information that they would not otherwise relinquish to an unfamiliar person. For example, an individual can post a message about an exciting topic, making it appear to come from a trusted 'friend,' and then link to a dangerous Website that aims to steal credit card data and other valuable information (Panda 2010, 6).

Offenders can also remain undetected by taking only small amounts of money from a large number of victims. Professor David Wall has used the term 'micro-fraud' to describe electronic victimizations that are informational, networked and globalized, which tend to be individually small in impact yet significant in their sum total (Wall 2010(a), 69). These frauds are typically considered too small to be acted on, and are often written off by victims (including banks) and/or not large enough to be investigated by police agencies. Wall reports that police tend to be reluctant to commit investigative resources to cases with losses of less than USD$5,000 to USD$7,000 and banks are typically willing to write off losses below USD$1,500. This is significant because most of the fraudulent schemes discussed have average losses, per victim, of under USD$2,000 (Wall 2010(a), 80).[14] Similarly, the 2008 National Survey on Fraud Against Businesses in Canada reported that a large majority of retail (89%) and banking (91%) establishments that had been victims of fraud in the previous 12 months reported suffering cumulative losses of CAD$20,000 or less due to fraud committed directly against them (Taylor-Butts and Perreault 2008, 16).

As Wall points out, such frauds tend to be "highly numerous yet relatively invisible" (Wall 2010(a), 80). Although the media tends to overstate the cyber-fraud problem, there is also the difficulty of under-reporting by victims (Wall 2010(a), 80). Incidents are frequently either un-noticed by victims, or not reported to anyone due to sheer embarrassment, or they may be reported directly to the bank and, thus, not appear as an official crime statistic (Wall 2010(a), 80). This means that offender and victim profiles are low because so few micro-frauds are never reported. As well, there is the problem that many micro-fraud incidents are committed across jurisdictional borders, which makes it more difficult for police to track the problem and respond to it. For the

[14] The average losses are reported as follows: non-delivered merchandise and/or payment ($800); internet auction fraud ($610); credit/debit card fraud ($223); Nigerian letter fraud ($1,650); identity theft ($1,000). These figures, cited by Wall, are based on 275,285 complaints received and 72,490 cases referred by the Internet Crime Complaint Centre in 2008 (Source: IC3, 2009).

most part, micro-frauds tend to be too small in impact to warrant the expenditure of police resources, even within local jurisdictions (Wall 2010(a), 80). Clearly, the most effective response to micro-frauds is a combination of technological and education solutions, including ensuring that individual computer users make their systems more secure and remain on the lookout for scams. However, as Wall points out:

> A major problem experienced to-date in policing the micro-frauds that result from the likes of scareware has been has been the lack of an effective, consistent and easy reporting system. This has long meant that crucial strategic intelligence which identifies 'the bigger picture' of impact at a national level has been lost, as has the important tactical criminal intelligence relating to the offenders, which hampers the police ability to investigate (Wall 2009, 64).

It is important that organized cybercrime groups are decentralized and do not provide a single target or point of failure for law enforcement, largely because they rely on many different actors in various countries, particularly within unregulated environments (Etges and Sutcliffe 2008, 91). The global nature of these organizations, and the fact that they are constantly changing geographic location, increases the difficulty of locating the perpetrators behind their operations and shutting them down (Symantec 2009, 56). The Internet also provides more secrecy and anonymity than any real-world physical environment. The non-hierarchical and network-based structure for coordination and cooperation is ideally suited for criminals in the digital age. This is evidenced by the increased number of computers used to perpetrate crime remotely (i.e. 'bots').[15] The online underground economy also provides global opportunities for the distribution of intangible goods (e. g. malicious software code and stolen identity information) and specialization in individual products and services (e.g. network and application attack vectors, data hiding, financial fraud, identity theft, credit card fraud, and others) (Etges and Sutcliffe 2008, 92). To combat these sophisticated and network-based criminal structures operating on the Internet, governments must form coalitions between law enforcement, government agencies, private sector organizations, NGOs, and professional organizations across jurisdictional boundaries (Etges and Sutcliffe 2008, 93). Combating cyber-fraud is a perfect example of where financial intelligence and interaction between public and private sectors is required (Gottschalk 2010, 268).

4.0 Cyber-Fraud Legislation in Canada and Elsewhere

4.1 The Canadian Legal Framework

One of the challenges currently faced by legal authorities is the difficulty of applying existing legislation to criminal activities involving new technologies. Legislating in this area is faced with the complexity of protecting consumers and encouraging e-commerce growth without placing unnecessary restrictions on the trans-border flow of data (Davis 2003, 208). The *Criminal Code*

[15] Bot computers are computers that have been deliberately infected with a virus that allows the criminal to control certain functions of the computer without the knowledge of its owner. These computers can be used to launch coordinated attacks or to disseminate spam email messages for the purpose of perpetrating the fraudulent schemes.

has long contained a provision targeting fraud at s.380. Prior to the enactment of the new identity theft legislation (discussed below), the *Criminal Code* did not contain any specific identity theft offence. With the exception of the offences dealing with computers (s.342.1), and devices to obtain computer service (342.2), the Code offences relating to property and theft predate computer technology and the Internet.[16] There is also an offence in the Code which deals with mischief in relation to data (s.430); however, this provision has not been used to prosecute anyone in Canada for committing fraud or identity theft.

Bill S-4, *An Act to Amend the Criminal Code (Identity Theft and Related Misconduct)* received Royal Assent October 22, 2009. It created several new *Criminal Code* offences targeting those aspects of identity theft not already covered. Note that there was no identity theft offence prior to this. More specifically, it focused on the preparatory stages of identity theft by making it an offence to obtain, possess, transfer or sell the identity documents of another person. The key provisions of this legislation are as follows:

- **Clause 1** – Added section 56.1(1) to (4) of the Code - making, possessing, transferring, offering or selling "identity documents" of another person.
- **Clauses 4 and 5** – Added section 342(3) and 342.01 (1) of the Code - fraudulent use or possession or trafficking of credit card data and knowingly possessing, importing or exporting devices that can be used to fraudulently copy credit card data.
- **Clause 8** – Added section 368(1)(c) and (d) of the Code - using forged documents as if they were genuine, selling/making available forged documents, possessing forged documents with the intent to use it.
- **Clause 9** – Added section 368.1 of the Code - dealing in devices used to create forged documents.
- **Clause 10** – Added to the existing offence the fact of pretending to be another person to avoid arrest or prosecution or to obstruct the administration of justice. Defined 'personating a person' to include pretending to be a person or using that person's identity information as if it pertained to the person using it. For someone to be found guilty of identity theft, the prosecution must prove that he or she knowingly obtained or possessed another person's "identity information." Identity information is defined as "any information – including biological or physiological information – of a type that is commonly used, alone or in combination with other information, to identify or purport to identify an individual." The new s.402.1 of the Code gives examples of identity information. Also added section 402.2(2) of the Code - transmitting, making available, distributing, selling, offering for sale or possessing another person's "identity information" and amended section 403 of the Code, replacing the offence of "personation with intent" with identity fraud.

There are also a number of provisions in the *Personal Information Protection and Electronic Documents Act* (PIPEDA) that can significantly reduce the risk of identity theft and fraud by

[16] Note, though, that under s.342.1 of the Code, fraudulent use or interference with computer systems is an indictable offence punishable by ten years' imprisonment.

placing limits on the collection, use and disclosure of personal information. PIPEDA requires organizations engaged in commercial activities to adopt a number of safeguards with respect to the personal information they collect.[17] Both private and public sector organizations are also beginning to establish fraud control policies that address the risks associated with widespread Internet penetration in Canada. However, there needs to be further harmonization of these initiatives to deal with the problem of trans-border Internet fraud.

4.2 The Legal Framework in the United States

In the US, the regulation of electronic commerce, including the fraudulent activities discussed herein, generally fall the Federal Trade Commission (FTC), and to a lesser extent to the Department of Justice (DOJ), which can conduct criminal prosecutions and seek civil injunctive relief pursuant to 18 U.S.C. 1345 (Cukier and Levin 2009, 262). The US Constitution grants Congress the authority to supervise interstate commerce, of which electronic commerce, including spam, phishing, and other fraudulent activity committed over the Internet, is incorporated. There are a number of provisions within the *Uniform Commercial Code* which pertain to Internet fraud, including the following: *Access Device Fraud* (18 U.S.C. 1029) (i.e. fraud and related activity connected with access devices); the *Computer Fraud and Abuse Act* (18 U.S.C. 1030) (i.e. fraud and related activity in connection with computers); the *CAN-SPAM Act* (18 U.S.C. 1037) (i.e. fraud and related activity in connection with electronic mail; credit card fraud (15 U.S.C. 1644) and the *Identity Theft Assumption Deterrence Act* (i.e. 18 U.S.C. 1028) (i.e. fraud and related activity connected with identification documents, authentication features, and information).

In addition, the *Fair Credit Reporting Act* (15 U.S.C. 1681) was amended in 2003 by the *Fair and Accurate Credit Transactions Act*, with specific sections designed to combat identity theft. For example, the law requires credit agencies to correct erroneous charges within four days of receiving a police report and, in addition, credit agencies must take extra steps to verify an applicant's identity when a fraud alert has been placed on a consumer's file (White and Fisher 2008, 5). The *Gramm-Leach-Bliley Act* (1999) contains a section dealing with fraudulent access to financial information, requiring financial institutions, such as banks and investment companies, to have policies procedures and controls in place to prevent the unauthorized disclosure of customer financial information (White and Fisher 2008, 5). Lastly, the FTC was created by Congress, through the *Federal Trade Commission Act*. The Act, and subsequent legislation,

[17] PIPEDA requires organizations to comply with ten principles set out in the Model Code (Schedule 1), which include: collection limitation (the parties should limit how information is collected and collection must be with consent and knowledge that the information is being collected); data quality (the data must be accurate and relevant); purpose specification (the party must specify the purpose for which the information will be collected); use limitation (once information is collected for one purpose it cannot be used for another purpose unless the individual consents or this is authorized by law); security safeguards (the information must be secured from risk, e.g. from attacks by hackers); openness (transparency i.e. the individual should know what is being done with her information); individual participation (the individual should have access to her information and be able to look at it and correct inaccuracies); and accountability (there must be an oversight mechanism). Note also that *PIPEDA* imposes limits upon how long an organization can retain personal information. This means that even if personal information is collected with the consent of the individual, it cannot be stored in perpetuity. This helps to reduce the risk of identity theft by making it clear that organizations should get rid of information that they no longer need.

provide the FTC with its authority and allow it to regulate various aspects of e-commerce, issue orders, levy fines, and commence litigation against individuals and corporations (Cukier and Levin 2009, 262). The FTC also, through its general prohibition against unfair and deceptive conduct, enforces corporate policies against companies that fail to follow their own stated policies, even in the absence of relevant legislation.

4.3 British and Australian Legal Frameworks

In the UK, the *Fraud Act* (2006) came into force on January 15, 2007 and includes fraud by false representation, failing to disclose information to the detriment of the other person, and abuse of position for dishonest gain. In Australia, a project was established by the Model Criminal Code Officers Committee of the Standing Committee of Attorneys-General which comprised senior law officers from all jurisdictions in 1990. The Commonwealth enacted general Model Criminal Code principles of criminal responsibility in Chapter 2 of the *Criminal Code Act 1995*, and subsequent amendments have added substantive provisions. These include theft, fraud and other property offences, forgery, bribery and offences against Commonwealth public officials. The *Cybercrime Act 2001* came into effect in October 2001, adding new provisions to the *Criminal Code Act 1995, the Crimes Act 1914* and the *Customs Act 1901*. The *Cybercrime Act* served to modernize Commonwealth computer offences and provided a model for the states and territories (Urbas and Choo 2008, 20).[18] The *Crimes Legislation Amendment (Telecommunications Offences and Other Measures) Act (No.2) 2004* added Part 10.8 – Financial information offences to the *Criminal Code Act 1995*. This contains offences directed at dishonest dealings with personal financial information or use of devices (such as credit card skimmers) to obtain such information without consent (Urbas and Choo 2008, 20). The *Spam Act* (2003) makes it an offence, punishable by civil penalties such as large fines, to send bulk unsolicited email in Australia or to Australian recipients (Urbas and Choo 2008, 20).

5.0 Jurisdictional Issues Related to the Investigation and Prosecution of Cyber-Fraud

A number of important jurisdictional issues stem from the cross-border nature of cybercrime. These include limited law enforcement capacity in the face of rapid globalization and technological change, tensions from the conflict between national sovereignties, and the importance of international cooperation (Gabrosky 2006, 275). The following is a list of key jurisdictional associated with the complexities of cyber-fraud:

- jurisdiction (whether jurisdiction exists and the problem of concurrent jurisdiction);
- legislative difficulties associated with differing criminal law regimes (the requirement of dual criminality);
- managing strategic alliances and partnerships and ensuring the confidentiality and flexibility of responses (particularly in relation to the private sector);

[18] Subsequently, this model (for the enactment of cybercrime legislation) was adopted by a number of states and territories.

- dealing with differing privacy regimes;
- achieving mutual assistance and strategic intelligence in a timely manner;
- the need to secure the cooperation and assistance of internet service providers (ISPs);
- the need for the trans-national search of computer data banks and the interception of communications; and
- difficulties with managing and coordinating extraditions (Urbas and Choo 2008, 8).

The trans-national nature of cybercrime challenges traditional conceptions of criminal jurisdiction because conduct no longer necessarily occurs entirely within the territory of a single sovereign (Brenner 2006, 190). For example, in 2000, the Love Bug virus, which was launched from the Philippines, infected computers in at least twenty countries (Brenner 2006, 190). The person who was alleged to have released the ILOVEYOU virus was never prosecuted for that act because the mischief was not defined under Philippine law at the time that it occurred, although it was prohibited in a number of countries impacted by the virus (Gabrosky 2006, 186).

Since cybercrime can transcend national borders and given that the activities of an offender often result in the commission of a crime in multiple countries simultaneously, attention must be paid to achieving the following goals on an international basis:

- the harmonization of substantive computer offences in national legislation;
- the harmonization of procedural provisions relating to the investigation and prosecution of computer crimes; and
- the establishment of cooperative measures facilitating the exchange of evidence, information and the extradition of suspects (Schjolberg 2008, 1).

It is encouraging that the global threat of cybercrime has triggered the response of international agencies and law enforcement agents around the globe. Indeed, there have been new coalitions formed by law enforcement, government agencies, NGOs, and private sector actors, to address the transnational nature of cybercrime. Canada is an active participant in a number of international organizations, such as the G8 Group of Senior Experts on Transnational Organized Crime, the Committee of Experts on Crime in Cyberspace of the Council of Europe, and the Organization of American States Group of Government Experts on Cyber-Crime. The Government of Canada hosts global summits, conducts international studies, and helped draft the Council of Europe's *Convention on Cybercrime*. The Canadian Association of Internet Providers is currently sharing information with European ISPs and working with other countries to develop international solutions.

Interpol, which is an international law-enforcement organization with 188 members, has been at the forefront of an organized international response to online fraud for many years. The General Secretariat continues to offer specialized assistance to national law enforcement authorities in its member countries through a range of operational support, database services and police training. Interpol is also engaged in developing strategic partnerships with other international law enforcement organizations and public sector bodies. For example, the Interpol Counterfeit Payment Cards Database was specifically created to promote successful collaboration on a global scale. Interpol regularly hosts meetings of its Advisory Group on Payment Card Fraud, which is comprised of senior investigators and forensic experts from many member countries, as well as major credit card companies such as Visa, American Express and MasterCard.

In recent years, there have been a number of milestones that address the challenges of combating trans-national cybercrime. One of the most significant of these was the Council of Europe's *Convention on Cybercrime* whose efforts to harmonize substantive and procedural law serves as a model for nations around the world. This was the first multilateral treaty aimed at facilitating international cooperation in the prosecution of computer crimes. It was signed in Budapest on November 23, 2001, by member states of the Council of Europe and by several non-member states, including Canada, Japan, South Africa and the US, that participated in its development (Huey and Rosenberg 2004, 597). The Convention entered into force on July 1, 2004. As of March 16, 2011, there were 47 signatory states.[19]

Of the 47 countries that signed the Convention, 30 countries have ratified it and entered it into force, including the US. Canada has not ratified the Convention. The Convention requires each signatory state to make it an offence to commit certain crimes using computer systems (including computer-related fraud and forgery, offences related to child pornography and the infringement of copyright) and to grant new powers of search and seizure to its law enforcement officials, including the expedited preservation of stored computer data, search and seizure of stored computer data and the real-time collection of computer data. Article 25 requires law enforcement officials in each signatory state to assist those in other participating states by cooperating with "mutual assistance requests" from police "to the widest extent possible."

Elsewhere in the world, regional organizations have begun to address the important unresolved issues relating to trans-national cybercrime. Beginning in the late 1990s, the G8 subgroup on high tech crime established a 24/7 network of experts to assist in high-tech crime investigation to ensure that no criminal receives a safe haven anywhere in the world (Schjolberg 2008, 13). The G8 also negotiated principles and an action plan to combat high tech crime, as well as better practices documents, including guides for security of computer networks, international requests for assistance, legislative drafting, and tracing networked communications across borders (Urbas and Choo 2008, 12). In addition, the G8 has worked on training conferences for cybercrime agencies from every continent (except Antarctica) and conferences for law enforcement and industry on improved cooperation and tracing online criminal communications.

Similar steps have also been taken by the Organization for Economic Cooperation and Development (OECD). In 2002, the OECD published its *Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security*, which were developed with the following aims: promote a culture of security among all participants as a means of protecting information systems and networks; raise awareness about the risk to information systems and networks, as well as the policies, practices, measures and the need for their adoption and implementation; foster greater confidence among all participants in information systems and networks and the way in which they are provided and used; and create a general frame of reference that will help participants understand security issues and procedures for the security of information systems and networks. (Urbas and Choo 2008, 10).

[19] Council of Europe Treaty Office, available online at: http://conventions.coe.int.

The European Union (EU) adopted a Framework Decision and entered it into force in 2005, which provides that states will criminalize illegal system interference and illegal data interference, and illegal access to information systems (Urbas and Choo 2008, 15). Similarly, the Asia Pacific Economic Cooperation (APEC) has committed to encouraging its member states to enact a comprehensive set of laws relating to cybercrime, as well as a policy framework that addresses substantive, procedural and mutual legal assistance measures, consistent with international legal instruments (Urbas and Choo 2008, 16). APEC has conducted a capacity-building project on cybercrime for its members in relation to legislation and investigative capabilities, whereby the advanced APEC economies support the less advanced in training law enforcement personnel (Li 2007). Similar commitments were also made by the Association of Southeast Asian Nations (ASEAN) in 2006, and the League of Arab States, as well as some members of the African Union. As well, in 2008, NATO opened a centre for excellence on cyber defense in Estonia, in order to conduct research on cyber warfare. The Organization of American States (OAS) has also taken steps to combat threats to cyber-security, including urging member states to adopt cybercrime laws and to facilitate international cooperation.

The connection between organized crime and cybercrime was one of the focuses of the 11th UN Crime Congress in 2005. The United Nations General Assembly has also adopted a number of resolutions on combating the misuse of information technologies. A UN Working Group on Internet Governance was established to contribute to the World Summit on the Information Society which was held in Tunisia in November 2005 (Schjolberg 2008, 10). A Global Cyber-security Agenda was also launched in May 2007 by the Secretary General as a global framework for dialogue and international cooperation in the development of strategies and solutions to enhance information security. Additionally, the International Telecommunications Union (ITU) in Geneva has become the most active UN organization aimed at reaching harmonization on global cybercrime legislation and it has been looking at how to promote international cooperation and build on existing international agreements in this area, particularly the Council of Europe's *Convention on Cybercrime (*Schjolberg 2008, 20).

The private sector has also been active in trying to enhance the ability of law enforcement officials around the world to deal with the problem of cybercrime. For example, Microsoft has invested millions of dollars in developing an international training program and technological resource for law enforcement agencies around the world to better investigate computer-facilitated crimes against children (Microsoft 2005). This project was initially developed with the help of several international police agencies in conjunction with the RCMP and the Toronto Police Service (RCMP 2005)**.** While it has primarily been used to combat online child pornography, it can also be used to facilitate the investigation and prosecution of other kinds of offenders, such as those committing fraud and identity theft. Successes such as these indicate that the global fight against transnational cybercrime is capable of being won.

6.0 Additional Issues for Law Enforcement and Prosecutors

In Canada, the Royal Canadian Mounted Police (RCMP) is responsible for the investigation of all computer crime offences within its jurisdiction, as well as those in which the Government of Canada is victimized, regardless of the source of the offender, as well as offences involving organized crime or affecting the interests of Canada. Commercial crime sections of the RCMP

operate in every major city throughout Canada and include at least one investigator trained in the investigation of computer crime. These initiatives are further supported by the RCMP High-Tech Crime Forensics Unit in Ottawa. Technical guidance and expertise is also offered by this unit to all Canadian police departments and federal government agencies with respect to computer and telecommunications crime investigations.

However, as noted, the anonymous nature of the Internet presents a significant problem for both law enforcement officials and victims because as many as half of victims do not know how their personal information was obtained. Offenders often mask their identities and are able to 'loop' or 'weave' their attacks through servers located in multiple jurisdictions. Electronic impersonation, otherwise known as 'spoofing', can also help to obscure the attacker's identity, as do anonymous remailers, and the encryption of digital information. This has an enormous effect on both the police response to identity theft and fraud, which are interrelated. Official crime statistics about online fraud display just the tip of the iceberg, as such, developing a comprehensive and proactive law enforcement response is extremely difficult (Blanco, Hache and Ryder 2011, 40).

In addition, the lack of coordination in handling complaints, even between agencies within the same jurisdiction, poses significant problems because individual incidents can be relevant to a wide range of agencies and may result in information being recorded at federal, state/provincial, and local law enforcement agencies, as well as credit reporting agencies, financial institutions, and regulatory agencies (Smith 2008, 381). This results in an inefficient backlog of relevant data and, given than many agencies do not coordinate and share intelligence, it is hard to tell if a complaint is linked to a single incident or to a series of incidents.

Individual victims typically do not find out that they have been targeted by identity thieves until they apply for a job, mortgage or loan; or they discover fraudulent charges on their bank statements or are contacted by credit agencies; or they are notified through proactive business practices (Smith 2008, 381). Recent research indicates that more than 80% of identity theft victims discover the theft from a negative experience (e.g. getting turned down for a loan), not through proactive business practices, by this point, the victim has already incurred some form of loss from the incident (White and Fisher 2008, 8).

While some discover the theft within thirty days, many victims do not learn that they have had their identities stolen for months or even years after the incident occurred (White and Fisher 2008, 8). Clearly, the more time that passes between the victimization and the discovery of the theft, the more difficult it is for the offender to be identified and located. Longer delays are associated with greater financial losses for the victim and more efforts to clear his or her name (White and Fisher 2008, 8). They also make it less likely that the victim will report the incident to anyone. Indeed, current estimates indicate that nearly 40% of identity theft victims do not report the crime to anyone (White and Fisher 2008, 8). Victims may believe that there is inadequate proof or that the matter is not serious enough to warrant police attention, or that nothing can be done. When corporations are victimized, the reasons for not reporting often include the fear of reprisals or that the publicity of security vulnerabilities could result in a loss of business or damage to their reputation (Smith 2008, 387). Furthermore, when the information is only reported to a bank or credit card company, it may not be relayed to police, which means that it will not be identified as an official fraud or identity theft-related crime statistic (White and Fisher 2008, 10).

7.0 Estimations of the Hidden Population of Cyber-Fraud Offenders

The problem of an unknown or hidden population of offenders is apparent in terms of law enforcement, resource allocation, criminal justice policy formation, and for criminological theory (Rossmo and Routledege 1990). In order for an incident of cyber-fraud to be recorded as an official crime statistic, the victim must report the event, the police must follow up on the report, and the case must be formally recorded. In terms of cyber-fraud specifically, it is difficult to get an accurate picture of the nature and frequency of victimizations because victims are often unaware that they have been targeted or do not report the crime for other reasons, including the perception that the incident is too minor to warrant further inquiry by the police. Given these problems, a number of approaches have been developed to reveal hidden populations of offenders through data mining. A form of capture-recapture that has been successfully used with other criminal populations is the best place to begin looking at this unknown category of offenders.

Capture-recapture methods are useful as a data mining tool for a number of different populations. In a nutshell, capture-recapture methods provide an estimation of population size and can be considered a variation of a general linear model (Weaver and Collins 2007). Traditionally, capture-recapture requires two samples and it creates a proportion based on sample members that are common to both to generate a hypothesized sampling distribution. These methods are contingent upon reoccurring patterns in observed data to make inferences about the proportion of a population that is active but unobserved in the data (Bouchard 2007). Capture-recapture methods were originally developed in biology to estimate the size of animal populations (Seber 1973), but have received some use for the study of human populations through epidemiological research.

Capture-recapture models have been used extensively in the field of substance abuse to estimate the prevalence of drug users amenable to treatment in a variety of communities (Bohning, 2004).[20] Capture-recapture methods have also been used within criminological research. Analyses conducted by Willmer and Greene and Stollmack on general populations of offenders demonstrated the first use of capture-recapture within the field of criminology. Following these initial attempts, researchers also used capture-recapture methods to estimate populations of burglars (Riccio and Flinkestein 1985), car thieves (Collins and Wilson 1990), prostitutes (Rossmo and Routledge 1990), and their clients (Roberts and Brewer 2006), illegal gun owners

[20] See also Calkins RF, Atkan GB (2000) Estimation of heroin prevalence in Michigan using capture-recapture and heroin problem index methods. *J Drug Issues* 30:187–204; Hser Y (1993) Population estimation of illicit drug users in Los Angeles county. *J Drug Issues* 23:323–334; Choi Y, Comiskey C (2003) Methods for providing the first prevalence estimates of opiate use in Western Australia. Int J Drug Policy 14:297–305; Hickman M, Cox S, Harvey J, Howes S, Farrell M, Frischer M, Stimson G, Taylor C, Tilling K (1999) Estimating the prevalence of problem drug use in inner London: a discussion of three capture–recapture studies. *Addiction* 94:1653–1662; Smit F, Toet J, van der Heijden P (1997) Estimating the number of opiate users in Rotterdam using statistical models for incomplete count data in *European Monitoring Centre for Drugs and Drug Addiction (EMCDDA), 1997 Methodological Pilot Study of Local Prevalence Estimates*. EMCDDA, Lisbon; Brecht M-L, Wickens TD (1993) Application of multiple-capture methods for estimating drug use prevalence. *J Drug Issues* 23:229–250.

(van der Heijden et al. 2003), and drug dealers (Bouchard and Tremblay 2005). Due to the inherent nature of criminal offending, capture-recapture methodologies require expansion in order to satisfy two key assumptions: population homogeneity and independence.

The problem is that the two-method sample requires that no outside variables influence the actor's inclusion (or lack thereof) in the second sample: the cases must be independent of one another across samples (Weaver and Collins 2007). This might be problematic for current efforts in the case where, for example, an offender who was caught would subsequently attempt to not be caught a second time. Similarly, the two samples must be homogenous to the extent that there is no structural reason why a particular case is more likely to be captured more than an alternate case. Given the variability across cases of cyber-fraud, it is unclear how homogeneity could be achieved. Valuable insight into minimizing the effect of these potential assumption violations was generated through pioneering work into the use of capture-recapture in identifying unobserved drug cultivation (Bouchard 2007).

In general terms, a sampling distribution is all of the possible outcomes for a statistic. While a normal distribution, sometimes called the bell curve, is appropriate for some types of data, this is not always the case. For example, consider a situation in which the goal is to estimate a distribution of the number of traffic violations. While it might be possible to find records for those with one, two or three traffic violations, there is no record for those with zero violations (Rider 1953). In terms of measuring cyber-fraud, a truncated discrete distribution would be a more appropriate representation given the difficulty of estimating the frequency of those who have not been arrested or re-arrested. Specifically, the truncated Poisson methods allow for prediction of a specific number of occurrences of an event in a specific period of time in which there is no information about the "zero group [which] is unobserved" (David and Johnson 1952). However, the Poisson distribution can be problematic when applied to criminal populations. This is because a general Poisson distribution requires that a number of assumptions must be made: the population under study must be closed; the population must be homogenous; and the probability for an individual to be observed and re-observed must be held constant during the observation period (Bouchard 2007). The first and second assumptions pose obvious difficulties. As suggested by Bouchard, "[o]ffenders tend to go in and out of offending at different periods of their lives; some are more active than others, and they may trigger different probabilities of arrest and re-arrest" (Bouchard 2007). More importantly, perhaps, the third assumption is problematic for criminal populations as offenders have the capacity to learn from their mistakes and modify their behavior following arrest and/or they might be subject to increased monitoring and targeting following an arrest (Bouchard 2007).

Bouchard has demonstrated that the use of truncated Poisson methods such as the Zelterman estimator, which is specifically designed to withstand departures from these assumptions (Collins and Wilson 1990), provides an appropriate method for capturing hidden criminal populations. The estimator is given by:

$$Z = N / (1 - e^{(-2*n2/n1)})$$

Where Z is the total population, N is the total number of individuals arrested with a particular criminal charge, n1 is the number of individuals arrested once, and n2 is the number of individuals

arrested twice in a given time period (Bouchard 2007). Accordingly, if data on known arrests and re-arrests "follow the Poisson distribution specified by Z's model, the missing cell in the distribution should be estimated correctly, that is, the number of offenders with zero arrests" (Bouchard 2007). This approach allows for an assessment of hidden populations.

The advantages of Zelterman's Poisson estimator for the purpose of estimating criminal populations are evident. First, it can minimize the impact of population heterogeneity in arrest risks by eliminating the minority of high-rate offenders with multiple arrests. Specifically, the formula provided by Zelterman includes only those offenders arrested once (n1) or twice (n2) for the purpose of establishing the arrest rate parameter. As Bouchard comments:

> Zelterman (1988) and other researchers who derived similar models (Chao 1989), base their approach on the rationale that estimation models should be complex enough to be meaningful, but simple enough to contain only the parameters that are necessary, and close to the quantity to be estimated: Observations that are close to the object of interest should, intuitively, have more bearing on it. (Bouchard 2007).

Although this characteristic will result in more conservative estimations, there is some logic in the notion that information about offenders who are not arrested might be best estimated from information about offenders who are rarely arrested. It should be noted that more information is provided by using more complex models that consider the full range of arrestees and their different arrest rates (Bouchard 2007),[21] or models that consider a series of covariates in fitting an estimation curve (Bouchard 2007). [22]

A second advantage of Zelterman's truncated Poisson model is it can be used on only one sample (as with arrest data), which is in contrast to other capture-recapture approaches that require three or more samples to develop estimates. While this might be seen as a disadvantage in that there are instances in which triangulation would be advantageous for identifying a sample, the preferred method of estimating a hidden population of cyber-fraud offenders requires focus on those who are currently unaccounted for within the general population. Stated differently, using only arrest data confines the interpretation to prevalence estimates of offenders ''at risk of being arrested,'' which specifies the scope to those who are considered hidden (Bouchard and Tremblay 2005).

A possible concern associated with the use of Zelterman's truncated Poisson model is that the population of unknown cyber-fraud offenders cannot be assumed to be a closed population because there is a distinct possibility that offenders will enter and exit criminal activity. Despite this reality, the model assumes that "the hidden population of interest is a ''closed'' population" (Bouchard 2007). To overcome this problem, other researchers who have employed the Zelterman's truncated Poisson model have compensated through the use of data at an aggregate level. For example, in the identification of hidden populations of marijuana growers, Bouchard

---

[21] "Compared to the 30,298 index offenders estimated by Greene and Stollmack's (1981) heterogenous Poisson model for D.C. in 1975, the Zmodel derives an estimate of 29,842 offenders (a 2% underestimate)."
[22] "Compared to the 62,722 illegal gun possession offenders estimated by van der Heijden et al.'s (2003) Poisson-based regression model, the Z model derives a 50,866 offender estimate (a 23% underestimate)."

demonstrates that the "likelihood of severe departures from this assumption is minimized [with]… analysis of re-arrest distributions at an aggregate level (arrests and re-arrests at the provincial level) rather than at a city or neighborhood level" (Bouchard 2007). Although this does not eliminate the risk of desistance from criminal activity, aggregate level measurement does mitigate the chances of offenders "being excluded from the sample simply because they moved to another city or neighborhood" (Bouchard 2007).

There is also some evidence (Kendall 1999) that using closed models for open populations is not necessarily as problematic as might be first assumed. As is suggested by Bouchard, "if the period under study is short enough, criminal population movements are unlikely to be swift and massive enough to have an impact on the prevalence estimates" (Bouchard 2007) derived from closed population models such as Zelterman's. Given that Zelterman's truncated Poisson model has yet to be tested with a cyber-fraud population, and that the inherent 'non-spatial/non-geographic' component of cybercrime requires more investigation, it would be prudent to supplement the model with the use of hidden Markov models or others crafted for open populations. The selection of either or any data capture method is highly tied to the identification of specific population characteristics so that the most appropriate method is employed.

8.0 Establishing the Characteristics of Cyber-Fraud Offenders, Investigation and Networks

In academic discourse, a number of theories have been put forward to explain why people commit fraud. Some of the essential factors identified by researchers include the following:

- a perceived *opportunity*, such as the absence or bypassing of controls that enable fraud to be identified or prevented;
- an offender with a *motivation* to steal assets, whether through the existence of a financial crisis, the presence of debts, or living beyond one's means;
- a *rationalization* for acting illegally, such as the belief that the victim can bear the loss, or that the stolen funds will be repaid; and
- the absence of *capable guardians*, such as through inefficient business security practices, the absence of an effective regulatory framework, or a lack of effective fraud prevention resources and tactics.

The motivations and justifications for cyber-fraud are much the same. However, the Internet has created new opportunities for fraud, and offenders can relocate to jurisdictions where Internet Service Providers (ISPs) have trouble monitoring and filtering the increasing amount of traffic across their networks (Symantec 2010, 8). The Internet is a highly vulnerable domain, with few protections in the way of guardianship (White and Fisher 2008, 17). In addition, social networking sites continue to provide new opportunities for crime and some industry analysts have predicted that these venues will face new threats as the number of users continues to grow (McAfee 2010(b), 2). Users have proven to be highly trusting in these social environments and readily click on hyperlinks or other kinds of invitations to view content sent by their 'friends' (McAfee 2010(b), 4).

A number of other recent trends have increased the number and frequency of cyber-fraud incidents:

- an underground economy has evolved around stealing, packaging, and reselling information (Deloitte 2010(a), 5);
- individuals and organizations are increasingly dependent upon computer-based technologies for the storage and processing of information and communications;
- online banking, investing, retail and trade, as well as widespread intellectual property distribution, have created new opportunities for fraud and theft; and
- economic hardships resulting from the 2008-2010 global financial recession created new opportunities to exploit peoples' fears and economic vulnerabilities (Urbas and Choo 2008, 6).

For example, Symantec reports that while the levels of financially-oriented spam and phishing remained relatively constant from 2008 to 2009, there was a marked increase in messages advertising the refinancing of debts and mortgages, along with offers of loans and opportunities to earn money while working from home (Symantec 2010, 13). New job opportunities have also emerged within the ever more robust underground economy, such as the role of 'money mule' or 'wire mule,' discussed in subsection 3.0 (Deloitte 2010(a), 6). This demonstrates that cybercrime offenders have readily been able to adapt their techniques to take advantage of current events and significant economic trends.

As David Wall has discussed (Wall 2009), and as previously noted, the emergence of identified patterns and connections between those committing cyber-fraud has raised a number of questions about the relationship between network actors. In particular, cyberspace provides many kinds of criminal actors with a safe haven that also enhances their organizational and operational capabilities. Although a traditional network of organized offending has been considered, there is evidence to indicate that the hierarchical structure does not apply to online networks of cyber-fraud offenders. In other words, it would be hasty to assume such a simplistic understanding of the network structure without an identification of the prevailing structure itself (Morselli 2009).

Methodologically, the most suitable place to begin gathering data is through those who are currently engaged in combating cyber-fraud: law enforcement investigators and IT security professionals. Through the use of telephone interviews, data were collected relating to: the identification of criminal organizations; their membership; how leaders emerge; recruitment techniques; criminal activities; threat levels; and, joint task force strategies. Given that little is currently known about this particular hidden population of offenders, it is pertinent to explore the existing knowledge to ensure that the most appropriate research model is selected.

9.0 Methodology

A semi-structured interview method was used to gather information from the research participants. The questions were directed toward the potential for using innovative methodologies to estimate the scope of cyber fraud, to identify existing data sources and gaps, and to suggest novel sources of data that might help provide a more accurate picture of the degree of cyber-fraud in Canada. Further, possible ways to determine the proportions of cyber-fraud attributable to

criminal networks rather than single individuals were discussed. The interviews were conducted by telephone for approximately 45 to 60 minutes each.

The process of coding the interview notes was open-ended, whereby the notes were re-read with the understanding that themes corresponding with the interview guide would immediately be apparent (Esterberg 2002). The analysis also revealed additional patterns within the data that might also be considered thematic codes. The interview transcripts were then re-evaluated through focused coding which allowed for confirmation of the original patterns. While the original thematic coding revealed a number of characteristics about cyber-fraud prevention and enforcement, the focused coding generated patterns across the data sources that were unanticipated, particularly with respect to the differing perspectives maintained by the IT personnel when compared with those of law enforcement. The research findings were grouped into seven thematic categories that correspond with the focused coding methods.

9.1 Sample

Ten IT security and 9 law enforcement personnel from across Canada were interviewed. The interview group was generated through a purposive stratified sample of personal connections and subsequently a snowball technique was used to expand the sample. None of the research participants were known to the researchers prior to the interviews. Since interview participants were guaranteed anonymity and confidentiality, identifying codes were attached to the interview notes and none of the participants were identified by name. No remuneration was offered for participation in the study.

The IT Security personnel were from a number of different industry sectors across Canada. These included retail, banking/finance, university, food/restaurant, energy, and government. They were all senior level employees/executives with many years of experience in this field. The law enforcement personnel came from a number of different provinces and regions throughout Canada. They were also members of the RCMP and municipal police detachments in major cities throughout Canada. They all had experience with cyber-fraud investigations in their capacity as law enforcement officials in Canada.

9.2 Results

9.2.1 Methods and Means of Commission

The interview results show that there are many different forms of cyber-fraud being perpetrated in Canada and that the scams cover a wide range, from the relatively simplistic to the highly sophisticated. Respondents were asked what kinds of IT Security incidents involving fraud were most commonly encountered in last 12 months. One of the most frequently reported methods of attack was skimming through the use of a hand-held device or by altering the debit/credit card payment device at a point of sale terminal. In some cases, this was accompanied by the use of video recorders which were posted above the payment terminals to capture PIN information. These types of attacks were reportedly committed by “employees in many cases – not so much for pin pad replacements – remove ceiling tiles and install cameras…this could be cleaners or staff .”

Phishing attacks were also said to be common as was credit card theft and the fraudulent use of stolen credit cards to purchase goods and services. For example, one of the law enforcement participants commented that most of the offences known to him or her involved "scams where the person used a camera and a false pin pad to retrieve data – and videotape you entering your PIN – and then reproduce the cards and start using them" . Another kind of cyber-fraud reported by respondents was utilities fraud (with respect to an electrical utility). In terms of harm caused, one respondent pointed out that, "it doesn't pay anything to target us for financial means – we're afraid of attacks to critical infrastructure – causing outages".

It was also evident from respondents' responses that those perpetrating cyber-fraud scams have readily adapted their techniques to take advantage of current events and economic trends. Following the recent earthquake in Japan, for example, there was apparently an immediate circulation of fraudulent emails online requesting donations to help the victims. As was reported by one of the law enforcement respondents:

> [S]tarting in 2008, new scams related to the downturn in the economy – job scams, chat rooms, Websites – targeting people looking for work and money right away – small loans where you have to pay an advanced fee. Social networking sites or job sites, Craigslist, Kijiji are all significant. Mystery shopper is a new scam – targets are told to pose as customers at Western Union, often at a Wal-Mart outlet, and they have to go in and wire money.

A different participant within the law enforcement sub-sample commented on the evolution of the means by which cyber-fraud is committed, noting that:

> I can't believe how many times we have people coming in to lodge complaints about money sent overseas – now it's mostly emails not letters – people are being used as money mules to transfer money overseas. They're expecting to receive something back but they never receive anything. Also, people post ads trying to sell their cars on the Web and people from other countries ask them to ship the car overseas. Fortunately, most victims are smart enough to not do this but they report it through our Website as a tip as opposed to an official complaint.

Similarly, at tax time each year, there are fraudulent tax centre Websites set up that direct victims to enter their personal information, including social insurance numbers, to see if they will receive a tax refund. Additionally, individuals are frequently using cyberspace to advertise popular and trendy goods for sale that do not actually exist. An example of this type of activity was provided by one participant who commented on monetary losses sustained during the 2010 Olympic Winter Games in Vancouver, noting:

> There were about 26 victims (defrauded online through Craigslist and Kijiji) who were offered tickets to Olympic events. The offender took their money and then told them he didn't have any tickets – he was taking people's money with no intent of providing them with tickets. In general, most [of the victim losses] were less than $1,000.

Individual victims do suffer more costly losses. As was suggested by the same interviewee, "[i]n another case, a victim was out $30,000 which she paid up-front for a real estate rental – she was new to Canada".

9.2.2 Harm Caused to the Victim

Not surprisingly, the interviews with law enforcement respondents appeared to focus on the individual victims of cyber-fraud, whereas the IT sample was primarily concerned with the industries each represented. In one instance, when a law enforcement participant was asked how many of the instances of cyber-fraud were directed toward individuals, the response was succinct: "All of them".

In terms of harms, the same sample member elaborated suggesting that cyber-fraud had a smaller impact on individuals than on companies, commenting that:

> [M]ost bank cards can only retrieve $1,000 per day – so you're looking at mostly $3,000 max per 3 days for a bank card…if it's a credit card, the offender can purchase big ticket items (e.g. a television or stereo) or make long-distance phone calls.

This was especially true for individual scams that occur solely online, such as through a virtual classified ad, or the purchase of a product on the Internet, which generally tend to be minuscule in amount, frequently as little as $200. One of the reported reasons was that people tend to be more willing to overlook the warning signs and do not get suspicious or nervous if it is only a small amount.

The emphasis on individual victims of cyber-fraud was articulated by a different law enforcement participant who noted that we have a "tendency to think cybercrime happens in large cities but it happens across the country – victims are often rural… it is a country wide phenomenon…not just in Ottawa or large banks in Toronto".

A concern for the characteristics of the victims was also reported among the law enforcement sub-sample, such as when one participant commented that: "Many victims are older people – if they lose money, it's very hard on them (even just $1,000 or $2,000 – this affects their health, medication, food, etc.)" .

This finding was reiterated by a different participant who commented that:

> I haven't dealt with any corporate threats – most go to RCMP commercial crime section – what I see are threats to individuals – the elderly and the vulnerable are often victimized through email – the 'send us money scams,' or 'transfer money to this account' scams, etc. .

Another participant noted that there was little pattern in the victim type, commenting that: "victims are spread between male and female and across a wide range of ages".

Additionally, some organized crime groups reportedly keep the target amounts low to ensure that victims will not be inclined to complain and police will not be willing to investigate. Even for larger scams, such as romance scams through online dating sites which often get personal, and sometimes moves off-line, the typical price asked by scammers tends to be in the range of $3,000 to $5,000 (although this depends on the net worth of the victim). Generally speaking, this research shows that the amounts stolen tend to be under $5,000.

Yet, one of the IT personnel stated that for a secondary victim, such as a bank, these losses can add up to as much as $100,000 monthly, or $1.2 million per year. The participants also reported that there are a number of non-monetary harms that result from the cyber-fraud incidents they encountered. When the IT personnel sub-sample commented on the harms it was primarily in terms of administrative expenditures, both for preventing and responding to cyber-fraud occurrences after the fact. For example, one participant noted that there is an expense associated with the activities beyond any initial loss, citing:

> [O]perational impacts – general cleaning up of malware and anti-virus takes time. Keeping anti-virus software up to date, patches, vulnerability scanning, monitoring network traffic, scanning for vulnerabilities needing patches.

For corporate victims, harms also include reputational or brand damage and loss of customers. In the case of individuals, the non-monetary harms consist of emotional distress, embarrassment and powerlessness, damage to reputation, intimidation, stress and depression. In particular, romance fraud can leave devastating results behind – victims send thousands of dollars to people whom they believe to be their soul mate. In the most extreme form or romance scams, Canadian victims are lured to another country, and when they arrive, they are held hostage for ransom, which is demanded via the Internet.

9.2.3 Offender Characteristics

Among the IT sub-sample there appeared to be some disagreement as to the source of offending: was it the result of malicious outsiders or insiders? For example, one IT participant stated that individuals within the company are responsible for incidents “about 20% of the time”. A different IT participant noted that:

> Thefts are external but compromises – to pin pads and cameras – are mostly internal. There is a 400% turnover in the restaurant business, so it’s hard to keep tabs on the staff…but when hiring, our policy is to run credit and police checks.

The same participant also seemed to indicate some difficulty in preventing fraud from taking place internally, commenting that “[it is a] franchise business so it’s hard to enforce [hiring policies]…we have never caught an individual by running a police background check…this only covers people already caught by police” .

Interestingly, it was reported that an insider would be treated differently than an offender from outside the company, and it was reported that there may possibly be a link to organized criminal enterprises when an insider is involved. As was noted by one of the IT participants:

> If it's an employee, we call it insider fraud – a different classification. We have systems that forensically track this when it occurs – while it doesn't happen as often...[we] have experienced this in past 12 months. The traditional way is when an insider is approached by an external crime group (i.e. the employee works at the help desk and has access to customers' data).

Given the finding from the IT sample that insiders were commonly dealt with internally whereas outside cyber-fraud offenders were reported to the police, it was not particularly surprising that a number of the law enforcement participants reported that, in the case of corporate victims, offenders tend to be outside of the organization. For example, when asked about the location of offenders, one law enforcement participant commented that to the best of his or her knowledge, the offenders were "all outsiders". However, this was also the response given by other IT participants who identified the primary source of cyber-fraud as originating outside the company.

9.2.4 Network Structure and Function

Many of the law enforcement and IT security personnel believed that cyber-fraud incidents in Canada are being perpetrated by individuals operating within criminal networks. Among the IT sample, the assessment that cyber-fraud was tied to a network structure was made either based on the characteristics or perceived sophistication of the offence or based on information reported to the individual from an outside authority. For example, one participant reported that:

> …it was a pattern – when we saw the pattern of machines being stolen, it was easy to figure out that it was not just one individual doing it. Stores were broken into close enough in time that it could not have been the same person.

According to a different participant, it was not the characteristics of the offence but the magnitude. When asked about whether the cyber-fraud involved a criminal network, this participant responded:

> Yes, I believe so. A lot is instinctive because I believe some things being done are too large in scope for an individual to do. Even the unsophisticated attacks…I think they're using tools created by others. It seems unlikely that it's an individual effort. Seem to be sophisticated at the level of identifying targets but actually going after the targets is done by less sophisticated means.

Another IT participant reported a similar belief about the complexity of cyber-fraud schemes, indicating a network structure behind the offence, noting that "…the devices are sophisticated, so we assume they are organized...[especially when] other similar devices are popping up around the country" . In other words, the attacks are too large and sophisticated for an individual to carry them out alone, particularly when other similar kinds of attacks are occurring throughout Canada.

On the whole, the participants believed that offenders were working together in small groups of 2 to 3 people. Additionally, they reported that these individuals were not Canadian and, frequently, not operating from within Canada. For example, one participant noted that, "We're aware of those

– individuals and organizations – from the Russian mafia" . Reportedly, the primary means of detecting whether or not the individuals were located outside Canada was the fact that the IP addresses were traced to locations outside Canada. However, other participants indicated that they were under the impression that a criminal network was responsible for the cyber-fraud incident(s) they encountered because they were given this information from the police. For example, one participant noted that this was "what I've been told by the bank or the RCMP…the RCMP simply said they were part of an organized group".

Similarly, when asked whether the cyber-fraud incidents they encountered were committed by a criminal network, most of the law enforcement personnel we spoke with said yes. In some cases the participants reported a belief that the network structure was hierarchical. For example, one law enforcement participant noted:

> Yes. Often we see credit card skimming…a group of guys go out and steal a pin pad, then someone alters it with blue tooth technology; someone else goes and uses the card and physically gets the money. But I have little doubt there's people on top of these layers – they don't just work on their own.

This top-down structure was reinforced by another participant, who commented that: "If the individual is low-level and used to do fraud scams or to get money from one place to next, he will not know who is at the top".

Consistent with the existing research, cyber-fraud is reportedly being committed by small groups of individuals who are quite well organized, highly technically proficient, and who know what they are doing. According to the law enforcement sub-sample "they never act alone. They are in small groups, highly organized, and know what they're doing. They are often very well organized…always multiple people".

A different respondent reiterated this point, commenting that the specific network was disperse, and observed that the networks are:

> Loosely knit – not like structured traditional criminal networks. Don't know if they use real names or online handles. [They] communicate through chat rooms – they're restricted and you have to know someone. Most speak English or French – communicate in these languages or their mother tongue.

In general, a trend of disagreement about the form of the particular structure was noticed. In some cases, respondents reported that the networks also have connections with other, more traditional, criminal organizations, such as the Hell's Angels; yet, little was known about how they find these groups and make these connections. According to a different participant, the structure of cyber-fraud networks resembles the hierarchical, traditional structure: "If an individual is low-level and used to do fraud scams or get money from one place to next, he will not know who is at top. Individuals who work on creating scams are more privy to what goes on in the group". The most important players tend to insulate themselves with technology from the rest of the group, making it difficult for law enforcement to locate the true leader, or the person coordinating the movement

behind the group. The members of these groups are also reported to deal in counterfeit currency, fake passports and identification documents, as well as cyber-fraud.

There was evidence among the law enforcement sub-sample that the traditional hierarchical network structure was not necessarily evident as noted by one interviewee: "It's more like little companies and sometimes the company is one person – they have business relationships but [not the] traditional way of organized crime". When probed for additional explanation, the same interviewee commented:

> For example, if someone has a list of credit cards and personal information, he did it by himself then looks in chat rooms and forums to find others – these people can buy the list – but it's not organized crime, is like a client/provider relationship – not like Hells Angels who have the same pattern of selling drugs – these guys are not loyal to a provider and to clients…the people do business together but it's not well organized…they come together for transactions and have places where they share things – chat rooms, Websites – these are all virtual places .

It was also acknowledged that there is still a great deal of hyperbole and speculation in this area, even amongst law enforcement, and more studies are needed to gather information about the types of individuals committing cyber-fraud. The disagreement about the network structure was also recognized by one respondent who commented that "[They] hear stories, know some details but there are large amounts of rumour about who is running the groups. We need more effective studies on the types of criminals [that] we're dealing with".

Interviewees indicated that the network bases tend to be from overseas (Eastern Europe - Romania, Bulgaria, Poland and Russia - and the Middle East, East Asia and West Africa, including Algeria, China, Sri Lanka, Ghana and Nigeria, as well as the UK, Germany, Spain and France) and well educated, with a great deal of technical computing knowledge and expertise. Furthermore, along with individuals, companies are also targeted by cybercrime networks. As one interviewee commented: "Also, high-profile hacking and phishing Websites are at a higher level and these guys are good at hacking and also banking system knowledge".

The difficulty in identifying a cyber-fraud network structure might be a result of the diversity of law enforcement activities. As was noted by one participant:

> A lot of our investigations end up intercepting the middle group. Some police agencies tend to focus on the street level for quick arrests and this doesn't impair criminal organizations. But even if we move up line, we can only get to the mid-level. The true leader or person benefitting is insulated – overseas – coordinating movement.

Further, the knowledge about the specific network structure was reportedly a function of the crime type. When asked to elaborate, the same participant commented that the structure:

> Depends on the fraud type. Mass marketing fraud involves small groups, closely knit, [who] move from one scam to the next. For example, fraudulent car ads on auto trader one week, EBay scams the next week. But the general *modus operandi* is the same –

> fake Websites or the purchase/sale of fraudulent goods and services – but it changes from one site to another. The credit card scamming groups are focused on credit cards but when it comes to making counterfeit credit cards, they are not focused on one commodity…they move on whatever the demand is. Also deal in counterfeit currency, fake passports and identification documents – it depends on the commodity. Do participants change? Some groups do, depending on the fraud type. They can have connections with other criminal organizations – but I don't know how they find these groups and make these connections.

Reportedly, when it comes to high-profile hacking and phishing Websites, offenders are often working as part of a team of specialists, each of whom has a defined role within the network. The structure of the network is reportedly goal-oriented. As one interviewee noted, the structure is comprised of "[s]pecialists – one guy does phishing, tries to steal information, then the other guy takes the information to get money – it's a world of specialists. Some are good at creating credit cards, others are good at trying to get money from ATMs". The same participant also noted that the emphasis is on knowledge rather than other resources, commenting that "[s]ometimes they work together to maintain bots, but that doesn't mean they're doing business together – they share knowledge but not necessarily money or criminal activities".

One individual might commit the phishing attack itself, for instance, while another 'specialist' takes the stolen information and creates fraudulent credit cards, which a third 'specialist' then uses at an ATM to steal money from the victims' accounts. This research further shows that, in some cases, these individuals locate each others in chat rooms and Web forums; then, they come together to carry out individual criminal transactions. Furthermore, according to one law enforcement participant:

> [p]eople know each other. Not just online. When online, [they] exchange information on how to better themselves. These folks know each other in real space. We never get to the key player. Most are male between the ages of 20 and 35. A lot are bilingual and some are tri-lingual.

9.2.4 Enforcement Activities

In terms of addressing cyber-fraud, the IT sub-sample reported a trend towards promoting prevention rather than repairing harms after the incident. In particular, prevention appeared to be a function of awareness of what is taking place within the business community along with an understanding of the nature and characteristics of cyber-fraud. There appeared to be an acknowledgement that cyber-fraud is very industry-specific and technology is being used to address the problem in a proactive manner. As one participant commented:

> We spend a lot of time on general behavioral profiling so you can look at something and see that the customer is expected to behave in a particular way…if it's out of the norm, it becomes something we need to take a look at. We want to make sure people are working within systems and rules…they can also use it to determine if someone is doing something unusual or unexpected.

A different respondent noted that the awareness that a cyber-fraud incident was taking place was based on the observations of the staff that were in a position to observe the activities within the business. For example, according to this respondent, in the case of skimmers, "eventually someone sees them or blows the whistle". In other instances, as noted by one respondent:

> the displacement of tiles in the ceiling [to mount a camera] was noticed and the behaviour of certain people was off. .. Changing [the] pin pad triggered an alarm and rendered it inoperative – this is a security mechanism – because the problem is well known in our business…this is a standard protective mechanism. It really comes down to social engineering and being aware of what's going on in the store .

Interestingly, although there was little knowledge about criminal fraud networks among the IT respondents, one of the IT sub-sample members noted that: "If there are multiple frauds, [we] consider it a point of compromise".

In general, a number of the IT personnel observed that their organizations have increased their IT security measures and moved into the real-time detection of fraudulent transactions, such as through the use of specialized software programs and security analysts. A number of these industry players have also started performing better background security checks of potential employees, although, in the case of the retail industry, this is reportedly difficult to enforce with franchise operations. Another measure that some of the IT personnel suggested would be helpful is the use of biometric pin pads. While chip cards are apparently a major benefit, they are not a perfect solution to the problem of identity theft and fraud.

In relation to the current law enforcement techniques available to combat cyber-fraud, one participant noted that technological advances have actually created a problem. Specifically, the participant indicated a "concern about the ability to keep pace with technological advances…the increasingly diverse uses of technology". Further, the increasing mobility of technology seemed to also be an additional concern given that: "with smart phones, crime can be committed anywhere, multiple cities in a day…we're losing the ability to track devices".

Despite the common propensity for not reporting fraud to law enforcement officials, one respondent commented: "We report everything – police get involved when it's an individual crime". Whether or not the police have the resources to address all reports was unclear. As one law enforcement participant noted:

> [P]olice don't have the resources to handle these cases – there are way too many of these incidents happening – if the average Joe loses a few hundred dollars, this is not a top priority for us. More important cases, like murder, are being committed. There are way too many incidents and there's no way any agency can handle it.

Neither the lack of reporting nor the lack of resources for responding appeared to be the toughest problem facing the law enforcement activities. As one law enforcement participant commented:

> The biggest hurdle police have is getting information we need, email providers or ISPs are often out of the USA or elsewhere outside Canada and it is very hard to obtain info

> – unless it's a life or death issue– this is good for protecting people's privacy but it doesn't help investigations. Would lawful access help? I don't know if it would have teeth.

9.2.5 Problems with Data and Reporting

From the IT sub-sample, the key issues regarding reporting appeared to be linked to a belief that authorities either could not, or would not, be able to do anything about the cyber-fraud incident. As one participant noted, "what is the incentive for reporting it? In my experience that there's no follow-up from law enforcement and this can lead to cynicism, especially when we spend the effort to report and then it seems useless".

Other comments from the IT sub-sample participants reiterated this concern:

> I think in my interactions with police, they seem quite unconcerned about credit card fraud and don't want to investigate claims. They don't seem to have enough trained staff. Also, they spend most of their time on Internet child exploitation, so this resource pool is being used for something else. They need to hire and train more people.

This was also the case for a different IT respondent, who commented, for example:

> I had another incident, a personal one, involving the online sale of my car – I reported it to the RCMP and they referred me to PhoneBusters and I got an automatic message saying no one can talk to you because we get so many calls and I wasn't even able to leave a message. I felt totally helpless.

In some cases, the IT sub-sample indicated that companies would not be willing to cooperate with the police because of the public image of being an organization susceptible to fraud. This finding was reinforced by a participant who, when asked if his or her company reports cyber-fraud, commented, "No. But stories haven't hit the news. Haven't frightened customers away". Explained more succinctly by a different IT sub-sample member, the issue was that, for organizations, "these kinds of things we want to keep quiet because we don't want our names in the newspaper".

Other concerns related to the logistics of data collection and a lack of communication between data sources based in an inherently competitive business environment. As was mentioned by one participant:

> [W]hen organizations are breached, we are scared to share it with anyone else. We are tight-lipped, this is a point of pride – but we're all suffering breaches – yet there's a culture of a lack of sharing with others in the industry, so no one is learning from each others' mistakes. There needs to be an informal sharing [of information].

However, there was also evidence that the companies are not necessarily even collecting the data that would be useful for better insight into cyber-fraud. One participant noted: "We don't measure

it. We don't keep a metric but measure electronic attacks on firewalls and spam, software attacks (99% of email we receive is spam or dangerous email containing viruses) but we don't track things on case by case basis".

In other cases, respondents asserted that even if data were available, it was doubtful that it would be put to any timely and practical use. As one of the IT participants notes, "[there is] little interest in pursuing white collar crime and fraud. We don't have statistics to make a compelling argument that cyber-fraud should be pursued – is cyclical – not a priority – industry is not reporting, don't want to tell story… and most [law enforcement] time and energy devoted to online child exploitation".

A key concern among the IT sub-sample seemed to be a lack of cooperation between industry and government. As was mentioned by one participant, "in dealing with the federal government…we have to provide them with information and don't always get it back. Assume nothing is being done. This disconnect is not helpful". When asked to elaborate, the respondent commented:

> From banks getting together and discussing this, we found out that federal Canadian law enforcement is pretty useless in terms of trying to be current on cyber-fraud threats. Often alerts are sent to us through CBA (Canadian Bankers Association) but there's no value in that because it's too late. The information is always released a week after we already know about the scams.

Among the IT sub-sample, problems with reporting were also constructed in terms of a cross-border comparison with the US. According to one respondent:

> Law enforcement is unable to help in any aspect of this. We need to bring information to law enforcement, but if it's low dollar amount (under $100,000), law enforcement are not interested in pursuing it. How do I know they're not interested in pursuing these cases? They're overwhelmed and have stated this to us. In the United States, law enforcement is more willing to assist with lower dollar amounts. Not sure if it is a capacity or a knowledge issue.

Respondents reported that more reports are submitted to regulatory bodies, such as the Securities Commission, the Competition Bureau and the Canadian Anti-Fraud Centre than the police. As one participant commented, "there is no policy on reporting to RCMP, just a practice of sharing with other companies. All major electrical companies in Canada are doing this". The same individual also made a comparison between practices in the United States and Canada, noting that in Canada there is "[n]ot as much regulatory compliance as in the United States – Ottawa doesn't regulate industry as heavily as in the United States. There banking and publicly traded companies are heavily regulated. It's not our government driving this stuff – it's more voluntary".

Furthermore, a number of banks and private companies have a security division and simply take care of the matter themselves. In other instances, reporting was seen to be an unnecessary cost for the business to incur. As was mentioned by one participant, "Security technologies are expensive and most organizations are not spending what they should in Canada. As a result, reporting and research doesn't happen". The trend toward non-reporting was not unanimous across the IT sub-

sample; indeed, others fully endorsed a system of mandatory reporting. As one participant commented, the "[the] private sector is blaming law enforcement and law enforcement is saying no reports are being made".

Like the IT sub-sample, when asked what are the key challenges related to reliably measuring the scope of cyber fraud and the number of associated offenders in Canada, the law enforcement participants reported that lack of education and information sharing are critical. In terms of reporting, there appeared to be awareness among the law enforcement sub-sample that minimal loss is a reason for the under-reporting of cyber-fraud. As one participant noted in relation to the data:

> I think there is…I don't know…I have no proof of this but I think people tend to file a complaint when there's a big loss. The number will be higher than expected because people with small losses don't report to police, just the bank. Mostly the banks refund money, so they don't need to report to police.

Further, the economic motivations for industry to not report cyber-fraud were identified by one of the law enforcement sub-sample members who noted that, "Perhaps banks are not [reporting cyber-fraud] because they don't suffer, it doesn't affect their bottom line" . The same participant also commented on the onus for companies to provide knowledge to the public, commenting that:

> Larger organizations – like ISPs or banks – or even agencies like INTERAC – they could be doing a better job of educating people. I think there could be more public safety alerts (like public service announcements) to remind people that banks don't send you emails…but so many people fall for phishing or pharming scams and don't realize big companies don't do business that way" .

Ultimately, there is a large gap in the data on cyber-fraud and the reason for this was identified by one law enforcement participant who stated that, "About 90% of all fraud data in Canada doesn't fit in police databases…the banks get reports, some are forwarded to police and some are just handled internally or dropped altogether. Pension and disability fraud is the same; it sits with organizations and doesn't get reported to police".

Individual victims are typically either too embarrassed or ashamed, or believe that the loss is not significant enough to justify making a report. As was noted:

> Not everyone files complaints, especially about identity theft – people don't call or notify police. A lot of the cyber-crime is not reported or is only reported to banks then is not reported to police by banks. They are afraid and want to keep it quiet – they want to protect their reputation and avoid negative publicity.

In terms of sharing information and data, like the IT sub-sample, the law enforcement respondents appear to offer evidence that this would be good practice. One participant commented that, "[T]here's a lack of sharing information. Not just law enforcement – the private and public sector too. The UK taught us that sharing of fraud data is crucial". This research demonstrates that there needs to be more emphasis placed on educating Canadians about how to avoid the scams themselves. The Canadian government, banks and ISPs must take greater responsibility on this

front. There should be more public safety alerts (i.e. public service announcements) to educate people on how not to fall victim to phishing scams.

One of the central frustrations was that cyber-fraud incidents are being reported to many different police organizations in Canada. The RCMP, municipal police forces and provincial police across the country all receive tips relating to cyber-fraud incidents. However, there seems to be little effort to coordinate these tips. Many seem to be kept internally and not reported to an external body. Many municipal police agencies do not report cyber-fraud incidents to the Canadian Anti-Fraud Centre, or any other entity. And, while reports are being made about violent and high-risk offenders through the RCMP, mandatory reporting does not apply in the case of cyber-fraud. Moreover, many law enforcement officials expressed frustration by the way that the statistical information is being recorded in the Uniform Crime Reporting Survey. According to the respondents, there is not enough specificity in the UCR reporting system when it comes to cyber-fraud, and cybercrime, more generally. The figures on cyber-fraud are lumped together under the heading of fraud, and there is no way to determine what type of fraudulent schemes the incidents are linked to. This means that information that could be valuable to better understanding cyber-fraud is being lost.

9.2.6 Suggestions for Data Sources and Solutions to Current Issues

One of the significant trends that emerged from the IT sub-sample supported mandatory reporting of incidents of cyber-fraud and argued for a standardized method of data collection. As was noted by one participant, "I think the way government is moving is in the right direction, creating RCMP offices, asking people to report to the RCMP; but more of these efforts are needed. When industry involved in an attack, we have to share information about it and having a federal framework to support this is very useful".

Further, the IT participants reported a need for information sharing within the IT security industry and a desire for government involvement in cybercrime fighting attempts. This was elaborated upon by the same IT sub-sample participant who suggested that:

> There needs to be a mechanism for the reporting and sharing of information to other members of industry…this would be very useful. There are good models for this elsewhere, like in the nuclear industry and air-traffic control…we need policy and regulations to enforce compliance. It's always easier with a public entity…it's easy to enforce compliance, sharing information, mitigating risks, but banks and telecoms are not in the same position. They are worried about losing customers…[in the electrical industry] we have a monopoly on customers. I don't see the same partnerships in the private sector, like banking.

Other participants reported a desire for IT accreditation, standardized reporting models, and government leadership to adopt models used in the United States. As was noted by one of the IT sub-sample members, "We need the Canadian government to step up…we see cybercrime units are being developed in the United States and this would be ideal here. I would be in favour of mandatory reporting legislation…the United States is the one to follow".

When asked what they thought could be done to improve reporting, a number of the IT sub-sample participants maintained that education and awareness are critical. In other words, Canadians must be made aware of what cyber-fraud is and where to report it. As one respondent commented: "[t]here's a number of different avenues for reporting: law enforcement at municipal/provincial/federal levels; PhoneBusters; federal organizations that deal with cybercrime related issues…but it's not clear who should be getting this information". Stated differently, many people do not know what to do when they receive fraudulent emails, let alone who to report to. On a more positive note, most of the IT sub-group participants affirmed that while not all companies are willing to cooperate with police, more openness and willingness to share information with police is strongly needed. As was noted by one participant:

> Generally, what we see is more United States-centric information…we're dominated by companies from the United States. I don't even know of a source of information specific to Canada (e.g. in terms of patterns and activity/information about attacks) where people volunteer information about attacks they've seen occurring. If we had a Canadian one, that would be extremely helpful…to know what kinds of attacks are taking place here…information specific to industries within our country…for us to understand what our defensive footing should be.

Many IT Security participants also strongly felt that there must be a more effective of sharing information about cyber-fraud, and cyber-security, more generally, between industry groups within a closed network of participants. As a participant commented, the process of sharing "is helpful and reassuring. It's helpful to know when you're not at the top of the list and being targeted". Taken together, the participants suggested that a Canadian body is needed to record and provide information about cyber-fraud attacks. There seemed to be a great deal of enthusiasm for a mechanism that would compel disclosure about cyber-fraud on a regular basis, something that emanates from government, which would collect information and then share it publicly. However, it was also suggested that the collection of data must be anonymous. It was further suggested that this kind of reporting and information-sharing mechanism would help with the lack of knowledge surrounding cyber-fraud within the Canadian context. As one participant suggested:

> We need stats within Canada, we need more research…Telus, Deloitte and PWC do good fraud and privacy surveys every year. People can fill out a survey online. Telus has been doing this for a long time. Every year, I'm invited to be part of focus group for what questions they should ask. These surveys are very useful to us – they allow us to do benchmarking and to see what the trend is for IT security management.

In the energy sector, statistical information about cyber-security, including cyber-fraud, is regularly shared with an RCMP liaison in Ottawa and then circulated back to the electrical companies. While it must be kept in mind that this close networking relationship is sponsored and enforced through the federal Critical Infrastructure initiative, it might be an effective prototype for cyber-fraud (i.e. to have individual liaisons in Ottawa to collect statistics about cyber-fraud from the various industry sector representatives and then report back the information to the various industry players). There was a great deal of support for this type of initiative; one participant

commented there was a "need for information specific to your industry and meetings to share information/collaboration about best practices. Some ability to participate in something like this would be useful".

When asked what might be done to improve the measurement of cyber-fraud in Canada, the law enforcement sub-group participants also provided a number of helpful suggestions. These ideas centered on a number of common themes, which included: money and resources; the Uniform Crime Reporting Survey; the need to encourage reporting and the sharing of information about cyber-fraud; and the establishment of a new national data hub with sophisticated data to measure and keep track of cyber-fraud incidents in Canada.

In terms of money and resource issues, the law enforcement sub-group participants focused on the need for more police officers trained to deal with cyber-fraud, particularly at the municipal and 'street' policing levels. Also, some respondents suggested that the federal government should be allocating more funds to municipal levels to deal with these problems, because they involve issues that could be conceived to be national security issues. This is currently a country-wide phenomenon and, as was reported, offenders are moving their operations from large urban areas to rural parts of Canada. Further, some respondents suggested that IT security responders need to be based in rural locations as well as the large Canadian cities. Moreover, this research strongly indicates that Canadian police cannot respondent to all fraud complainants, particularly when the perpetrators are located overseas and/or operating from an anonymous account, or where there is a need for information from email providers/ISPs outside Canada.

The research further revealed that there needs to be increased sharing of information about cyber-fraud among law enforcement agencies. According to the law enforcement sub-group participants, major ISPs could also be required to disclose information about cyber-fraud, as could private industry. The relationship between sharing information and the availability of resources for law enforcement was summarized by a member of the law enforcement sub-sample who commented that:

> Joint forces with police officers, banks, private companies are needed to share information. This kind of relationship is interesting; it can be a way of knowing more about the problem. But you need to guarantee anonymity. This is good for everyone – to share information anonymously.

There was also support for the IT suggestion of creating a mechanism whereby private and public industry players could anonymously disclose fraud losses to a centralized source. As one respondent offered, "reach people via the Internet. It's the easiest way to survey people. Increase inter-agency communication across the country – we need to encourage and foster this. We need links across Canada".

There also seemed to be a great deal of interest in finding a way to compel Canadian police agencies to exchange information about cyber-fraud and find out if groups are targeting multiple cities. This research demonstrates that the Canadian government would benefit from a national strategy for gathering data anonymously from police officers, banks, and private and public entities with respect to cyber-fraud. It is a matter of encouraging police agencies to communicate

with each other and persuading industry to report on what their actual losses are. According to the respondents, there is a great deal of support for mandatory reporting. As one respondent noted:

> I think if companies were mandated to report attacks, that might help - there have been cases of entire servers brought down and nobody knew anything. I think the spam laws that came into force recently (Bill C-28) should help Canadians, but the majority of spam originates from overseas.

According to the law enforcement sub-group, there needs to be a new way that Statistics Canada measures the police data relating to cyber-fraud in the Uniform Crime Reporting Survey (UCR) because the categories do not adequately reflect changes in society and in crime that have occurred over the course of the last decade. Currently, within the UCR scoring, there is no way to break down information about fraud by type, such as mass marketing fraud, or 419 scams, so it is not as useful to the police as it could otherwise be.

There was discussion about the creation of a central data hub to record and measure data relating to cyber-fraud across Canada. This entity could also conduct online surveys or polls of Canadians to gather information about cyber-fraud. Currently, the various police agencies across Canada have their own ways of collecting data and keeping track of files and many do not record complaints alone, preferring only to keep a record if the incident leads to a formal investigation. It would be more effective and efficient to create a centralized agency to collect and compile the data. Police agencies would be assured of better communication about cyber-fraud because the centralized agency could pass along the relevant information to the various law enforcement agencies throughout Canada. Having a central databank of known cyber-fraud offenders and cases across the country would also help with the identification of suspects in cyber-fraud cases and would enable researchers to map and measure the kinds of incidents that are commonly occurring.

According to the participants, a new national cyber-fraud tool used to collect data and effectively track cyber-fraud reporting would be beneficial. Since the majority of the information about cyber-fraud is either being funnelled to a variety of different organizations, including banks, regulatory agencies and various police organizations, or simply not recorded, intelligence units are needed to share this information with a national body that is able to consolidate all of the information about cyber-fraud into a centralized data hub.

10.0 Conclusion and Recommendations

Taken together, the issues and concerns raised in this report must be viewed as cyclical. The lack of reporting of cyber-fraud incidents by individual and corporate/government victims means that many cases are not being recorded as crime statistics. One likely consequence of this is that insufficient resources are being allocated to law enforcement personnel in this area because the true numbers of cyber-fraud victims in Canada are not being recorded and measured. Respondents suggest that cyber-fraud is not being viewed as a high enough priority such that insofar as adequate resources have not been provided to address the situation. This necessarily means that sometimes when victims come forward to the police, they are turned away because there are not enough resources capable of responding to their complaints. This leaves individual

and corporate victims frustrated and not wanting to turn to law enforcement for help or to officially report cyber-fraud.

At the same time though, many respondents suggested that there needs to be a more well-defined process and a single entity responsible for collecting cyber-fraud information. At the moment, there are too many different avenues for reporting – municipal, provincial, federal police as well as the Canadian Anti-Fraud Centre – it is not clear who should be getting the information. It was also recommended by respondents that there be an anonymous way to report to one body. Information about cyber-fraud appeared to be a concern for both respondent groups. The lack of training for law enforcement along with IT personal also seemed to be a concern. As was mentioned by a respondent from the IT sub-sample, "[a]n accreditation body for investigators (private IT investigators) would be useful. A governing structure – a professional organization – is needed for IT security".

Both the IT and law enforcement sources confirmed suspicions that both individuals and companies are not likely to report due to embarrassment and other reasons. While there were trends, many of the results were mixed. Some key patterns manifested across both sub-samples. For example, both the IT (excluding a minority of IT respondents) and law enforcement sub-section participants found that there is a lack of information about cyber-fraud in Canada and that something needs to be done about this.

Ultimately, a common belief was expressed among the interview respondents that there is a need for new policy measures to be developed to centralize a data collection source. As was suggested by both the IT and law enforcement sub-samples, anonymous surveys would elicit data from both individuals and companies who fail to report out of fear of embarrassment. In the case of companies, there is also support for mandatory reporting. According to some of the law enforcement sub-sample, standardization of reporting across law enforcement would also help to mediate the current weaknesses in the UCR Survey data. Further, respondents indicated that a lack of information hampers data collection, and that public awareness is critical.

In order to assess the scale of cyber-fraud in Canada, and how likely it is to change in the future, evidence must be gathered to document the scope and scale of the problem. Although some offenders operate from within Canada, there is evidence that many perpetrators are based in other countries. There is also some evidence of organized groups involved in cyber-fraud and in laundering illicit proceeds trans-nationally. The underground economy has also evolved into an increasingly mature global marketplace where technical skills and data can be purchased to carry out specific attacks. Symantec reports that readily available code kits, or crimeware kits, which are widely available for sale on the underground economy, are making it easy for novice attackers to compromise computers and steal information (Symantec 2010, 11). The task of determining, from limited data, the extent of cyber-fraud affecting a particular business sector, or even individual consumers, within Canada requires a far more sophisticated approach than has commonly been undertaken.

Due to the general lack of knowledge about criminal cyber-fraud networks, it would appear that the best source for data would be offender populations. This type of information would go a long way toward uncovering the true network structure of these hidden populations and thus help to

identify key players within the group. With the collection of preliminary data into cyber-fraud, the hidden population could be estimated through one of the standardized data estimation techniques discussed above. Of the options available for hidden populations, a truncated Poisson model is a good place to start. This would help to mitigate many of the issues confronted by law enforcement that lead to the lack of reporting and the inherent challenges that come with investigating and preventing cyber-fraud offending.

In summary, the following recommendations could be extremely effective toward addressing cyber-fraud in Canada:

- There needs to be more emphasis placed on educating Canadians about how to avoid the scams themselves. The Canadian government, banks and ISPs must take greater responsibility on this front. There should be more public safety alerts (i.e. public service announcements) to educate people on how not to fall victim to phishing scams.
- New initiatives, such as creating an online database of best practices which IT security professional members can add to and view, and/or developing an online community (e.g. to send out advice and tips) and holding best practice information sessions/conferences within specific industry sectors, could be instrumental to proactively responding to cyber-fraud threats, as well as gathering information about current threats and vulnerabilities.
- The Canadian government would benefit from a national strategy for gathering data anonymously from police officers, banks, and private and public entities with respect to cyber-fraud. It is a matter of encouraging police agencies to communicate with each other and persuading industry to report on what their actual losses are. There was support for the mandatory reporting of incidents of cyber-fraud and argued for a standardized method of data collection. In addition, there could be IT accreditation, standardized reporting models, and government leadership to adopt models used in the US.
- There is a need for more police officers trained to deal with cyber-fraud, particularly at the municipal and 'street' policing levels. Also, some interview respondents suggested that the federal government should be allocating more funds to municipal levels to deal with these problems because they involve issues that could be categorizes as national security issues. Cyber-fraud is currently a country-wide phenomenon and offenders were reported to be moving their operations from large urban areas to rural parts of Canada. Thus, IT security responders need to be based in rural locations as well as the large Canadian cities.
- There needs to be a new way that Statistics Canada measures the police data relating to cyber-fraud in the Uniform Crime Reporting Survey (UCR) because the categories do not permit for an analysis of types of cyber-fraud.
- A National data hub should be created to record and measure data relating to cyber-fraud across Canada. This entity could also conduct online surveys or polls of Canadians to gather information about cyber-fraud. A new national cyber-fraud tool could be used to collect data and effectively track cyber-fraud reporting.
- Since cybercrime can, and often does, transcend national borders, and given that the activities of an offender often result in the commission of a crime in multiple countries simultaneously, attention must be paid to achieving the following goals on an international basis:
    - the harmonization of substantive computer offences in national legislation;

- the harmonization of procedural provisions relating to the investigation and prosecution of computer crimes;
- and the establishment of cooperative measures facilitating the exchange of evidence, information and the extradition of suspects (Schjolberg 2008, 1).

- Resources are also needed to ensure that courts are equipped to deal with complex inter-jurisdictional fraud cases.

REFERENCES

Albanese, J. S. (2005). "Fraud: The Characteristic Crime of the Twenty-First Century." *Trends in Organized Crime 8*(4), pp.6-14.

An Act to Amend the Criminal Code (Identity Theft and Related Misconduct) Personal Information Protection and Electronic Documents Act S.C. 2000, c.5.

Begin, N. Dezhkam, N., Etges, R. and Hejazi, W. (2010a) "Managing the risk of social networking: Additional findings and analysis from the 2010 Rotman-TELUS Joint Study on Canadian IT Security Practices." Toronto: Telus Security Solutions.

– – – ., Dezhkam, N., Etges, R. and Hejazi, W. (2010b). "2010 Executive Briefing - Rotman-Telus Joint Study on Canadian IT Security." Toronto: Telus Security Solutions.

Berg, S. (2009). "Identity Theft Causes, Correlates and Factors: A Content Analysis," in Crimes of the Internet. Edited by Frank Schmalleger and Michael Pittaro. Upper Saddle River, NJ: Pearson Education Inc.

Hache, B., Carolina, A., and Ryder, N. (2011). "Tis the Season to (Be Jolly?) Wise-up to Online Fraudsters. Criminals on the Web Lurking to Scam shoppers this Christmas: A Critical Analysis of the United Kingdom's Legislative Provisions and Policies to Tackle Online Fraud," *Information & Communications Technology Law, 20*:1, 35-56.

B¨ohning, D., Suppawattanabodee, B., Kusolvisitkul, W, and Viwatwongkasem,C. (2004). "Estimating the Number of Drug Users in Bangkok 2001: A Capture-Recapture Approach Using Repeated Entries in One List." *European Journal of Epidemiology* 19, 1075-1083.

Bouchard, M. (2007). "A Capture–Recapture Model to Estimate the Size of Criminal Populations and the Risks of Detection in a Marijuana Cultivation Industry." *Journal of Quantitative Criminology*, 23: 221-241.

– – – . and Tremblay, P. (2005). "Risks of Arrest Across Markets: a Capture–Recapture Analysis of 'Hidden'Dealer and User Populations." *Journal of Drug Issues*, 34:733–754.

Brecht, M-L., and Wickens, T.D. (1993). "Application of Multiple-Capture Methods for Estimating Drug Use Prevalence. *Journal of Drug Issues*, 23:229–250.

Brenner, S. W. (2002). "Organized Crime? How Cyberspace May Affect the Structure of Criminal Relationships." (2002) *North Carolina Journal of Law and Technology, 4*(1):1-50.

Calkins RF, Atkan GB. (2000) "Estimation of Heroin Prevalence in Michigan Using Capture-Recapture and Heroin Problem Index Methods." *Journal of Drug Issues*, 30:187–204.

Campbell, D. S. (2002). "Focus on Cyberfraud." *Internal Auditor*, February: 28-33.

Canada. Criminal Intelligence Service Canada (CISC). (2010). "2010 Report on Organized

Crime." Ottawa: CISC.

– – – . (2005). Canadian Centre for Justice Statistics. "A Feasibility Report on Improving the Measurement of Fraud in Canada." Ottawa: Minister of Industry.

Canadian Anti-Fraud Centre. (2010)."Annual Statistical Report 2010 - Mass Marketing Fraud and ID Theft Activities" Available online at: http://www.antifraudcentre-centreantifraude.ca [accessed April 19, 2011].

Canadian Bankers Association (CBA). (2011). "Statistics." Available at: http://www.cba.ca/en/component/ content/publication/69-statistics [accessed April 9, 2011].

Chawki, M. (2009). "Nigeria Tackles Advance Fee Fraud." *Journal of Information, Law and Technology 1*. Available at: http://go.warwick.ac.uk/jilt/2009_1/chawki [accessed April 9, 2011].

Chellappa, R.K. and Sin, R. (2005). "Personalization Versus Privacy: An Empirical Examination of the Online Consumer's Dilemma." *Information Technology and Management*. 6 (2-3):181-202.

Choi, Y., and Comiskey, C. (2003) "Methods for Providing the First Prevalence Estimates of Opiate Use in Western Australia." *International Journal of Drug Policy, 14*:297–305.

Choo, K.K.R., (2008). "Organized Crime Groups in Cyberspsace: A Typology." *Trends in Organized Crime, 11*(3):270-295.

Collins MF, Wilson RM (1990) "Automobile Theft: Estimating the Size of the Criminal Population." *Journal of Quantitative Criminology, 6*:395–409.

Controlling the Assault of Non-Solicited Pornography and Marketing Act and Telephone Consumer Protection Act (the "CAN-SPAM Act), 18 U.S.C. § 1037.

Crimes Legislation Amendment (*Telecommunications Offences and Other Measures) Act* (*No. 2*) *2004*. No. 127, 2004.

Criminal Code of Canada R.S.,1985, c. C-46.

Cukier, W. and Levin, A. (2009) "Internet Fraud and Cyber Crime," in Crimes of the Internet. Edited by Frank Schmalleger and Michael Pittaro. Upper Saddle River, NJ: Pearson Education Inc.

Cybercrime Act 2001 No. 161, 2001.

David, F.N., and Johnson, N.L. (1952). "The Truncated Poisson Distribution." *Biometrics, 8*(4):275-285.

Davis, E. S. (2003). “A World Wide Problem on the World Wide Web: International Responses to Transnational Identity Theft.” Available At http://law.wustl.edu/Journal/12/p201%20Davis.pdf. [accessed April 19, 2011].

Dhamija, R., Tygar, J.D., and Hearst, M. (2006). “Why Phishing Works.” CHI '06: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, ACM Special Interest Group on Computer-Human Interaction.

Deloitte. (2010a). “Cyber Crime: A Clear and Present Danger”: Combating the Fastest Growing Cyber Security Threat. New York: Deloitte Development LLC.

– – – . (2010b). “2010 TMT Global Security Study – Key Findings – Bounce Back,” New York: Deloitte Development LLC.

Etges, R., and Sutcliffe, E. (2008). “An Overview of Transnational Organized Cybercrime,” *Information Security Journal: A Global Perspective, 17*:87.

Everett, C. (2003). “Credit Card Fraud Funds Terrorism.” *Computer Fraud and Security*, May:1-20.

Federal Trade Commission Act (15 U.S.C. §§ 41-58, as amended).

Gabrosky, P. (2006). “Editor’s Postscript,” *Crime, Law, Social Change*, *46*:275-276.

Gordon, S., and Ford, R. (2006). “On the Definition and Classification of Cybercrime,” *Journal in Computer Virology 2*:13-20.

Gottschalk, P. (2010). “Knowledge Management Technology for Organized Crime Risk Assessment,” *Information Systems Frontiers, 12*:267-275.

Gramm-Leach-Bliley Financial Services Modernization Act, Title V of the Financial Services Modernization Act of 1999, Pub. L. No. 106-102, 113 Stat. 1338 (Nov. 12, 1999).

Hilley, S. (2006). “The Shadowcrew – Organized, Yes, but ‘Organized Crime’?” *Infosecurity Today, 3*(1):10.

Hejazi,W., LeFort, A., Etges, R. and Sapiro, B. (2010). “The 2009 Rotman-TELUS Joint Study on IT Security Best Practices: Compared to the United States, How Well is the Canadian Industry Doing?” Corporate Hacking and Technology Driven Crime: Social Dynamics and Implications. T. Holt, B. Schell, eds. Hershey, PA: IGI Global.

Hickman, M., Cox, S., Harvey, J., Howes, S., Farrell, M., Frischer, M., Stimson, G., Taylor, C., Tilling, K., (1999). “Estimating the Prevalence of Problem Drug Use in Inner London: A Discussion of Three Capture–Recapture Studies.” *Addiction 94*:1653–1662.

Howard, R. (2009). Cyber Fraud: Tactics, Techniques and Procedures. Boca Raton, FL:

Auerbach Publications.

Hser Y (1993). "Population Estimation of Illicit Drug Users in Los Angeles County." *J Drug Issues* 23:323–334.

Huey, L. and Rosenberg, R.S. (2004). "Watching the Web: Thoughts on Expanding Police Surveillance Opportunities under the Cyber-Crime Convention," *Canadian Journal of Criminology and Criminal Justice 46*:597-631.

Identity Theft and *Assumption Deterrence Act*, Pub. L. No. 105-318, 112 Stat. 3007 (Oct. 30, 1998).

Ipsos Reid, (2009). "CSA Investor Index 2009." Prepared for Canadian Securities Administrators Investor Education Committee. Ottawa: Ipsos Reid.

Kendall, L.W. (1999). "Robustness of Closed Capture–Recapture Methods to Violations of the Closure Assumption." *Ecology, 80*:2517–2525

King, A. and Thomas, J. (2009). "You Can't Cheat An Honest Man: Making ($$$ and) Sense of the Nigerian Email Scams" in Crimes of the Internet. Edited by Frank Schmalleger and Michael Pittaro. Upper Saddle River, NJ: Pearson Education Inc.

Kowalski, M. (2002). "Cyber-Crime: Issues, Data Sources, and Feasibility of Collecting Police-Reported Statistics." Ottawa: Minister of Industry.

Lee, B., Cho, H., Chae, M., and Shim, S. (2010). "Empirical Analysis of Auction Fraud: Credit Card Phantom Transactions." *Expert Systems with Applications, 37*:2991-2999.

Levi, M. and Burrows, J. (2008). "Measuring the Impact of Fraud in the UK: A Conceptual and Empirical Journey." *British Journal of Criminology, 48*:293-318.

– – – . and Fleming, M. H. and Hopkins, M. with the assistance of Matthews, K. (2007). "The Nature, Extent and Economic Impact of Fraud in the UK." Report for the Association of Chief Police Officers' Economic Crime Portfolio. Available at: http://citeseerx.ist.psu.edu/viewdoc/ download?doi=10.1.1.108.8217&rep=rep1&type=pdf. [accessed April 19, 2011].

Li, X. (2007). "International Actions Against Cybercrime: Networking Legal Systems in the Networked Crime Scene." *Webology, 4*(3):1-45.

Longe, O.B., Wada, F., Anadi, A., Jones, C., and Mbarika, V. (2010). "Seeing Beyond the Surface: Understanding and Tracking Fraudulent Cyber Activities." *International Journal of Computer Science and Information Security, 6*(3):124-135.

Malm, A. and Bichler, G. (in press). "Networks of Collaborating Criminals: Assessing the Structural Vulnerability of Drug Markets."

McAfee. (2010a). “A Good Decade for Cybercrime: McAfee’s Look Back at Ten Years of Cybercrime.” Santa Clara: McAfee Inc.

– – – . (2010b). “2010 Threat Predictions.” Santa Clara: McAfee Inc.

Menn, J. (2010). Fatal System Error – The Hunt for the New Crime Lords Who are Bringing Down the Internet. New York: PublicAffairs.

Microsoft, (2005). “Tool Thwarts Online Predators.” Available at: http://www.microsoft.com /presspass/features/2005/apr05/04-07CETS.mspx [accessed April 7, 2011].

Morselli, C., Gabor, T., and Kiedrowski, J. (2010). “The Factors That Shape Organized Crime,” prepared for Research and National Coordination Organized Crime Division, Law Enforcement and Policy Branch, Public Safety Canada.

Morselli, C. (2009). Inside Criminal Networks. New York: Springer.

OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security (2002), available online at: www.oecd.org/dataoecd/27/6/2494779.pdf.

O’Neill, M. (2000). “Old Crimes New Bottles: Sanctioning Cybercrime.” *George Mason Law Review, 9*:237- 241.

Paget, F. (2009). “Financial Fraud and Internet Banking: Threats and Countermeasures.” Santa Clara: McAfee Inc.

Panda Security. (2010). “The Cyber-Crime Black Market: Uncovered.” Markham, ON: Panda Security.

Riccio, L.J., Flinkestein, R. (1985). “Using Police Arrest Data to Estimate the Number of Burglars Operating in a Suburban County.” *Journal of Criminal Justice, 13*:65–73.

Rider, P.R. (1953). “Truncated Poisson Distributions.” *Journal of the American Statistical Association, 48*(264):826-830.

Roberts, J.M., and Brewer, D.D. (2006). “Estimating the Prevalence of Male Clients of Prostitute Women in Vancouver with a Simple Capture–Recapture Method. *Journal of the Royal Statistical Society Series A 169:*1–12.

Rossmo, D.K., and Routledge, R. (1990). “Estimating the Size of Criminal Populations.” *Journal of Quantitative Criminology, 6*:293–314.

Royal Canadian Mounted Police (RCMP). “RCMP, Toronto Police Service and Law Enforcement from Across Canada Unite to Fight the Online Sexual Exploitation of Children - Microsoft Canada President David Hemler and National Police Services Join launch of Canadian-Developed Child Exploitation Tracking System (CETS),” Available at http://www.rcmp-grc.gc.ca/news /2005/n_0510_e.htm. [accessed April 19, 2011].

Schjolberg, S. (2008). “The History of Global Harmonization on Cybercrime Legislation – The Road to

Geneva". Available at: http://www.cybercrimelaw.net/documents/cybercrime_history.pdf. [accessed April 19, 2011].

Schwarz, C. J., and Seber, G. A. F. (1999), "A Review of Estimating Animal Abundance. III." *Statistical Science, 14*:427-456.

Sheehan, K.B. and M.G. Hoy, (2000). "Dimensions of Privacy Concern Among Online Consumers." *Journal of Public Policy and Marketing,* 19(1):63-73.

Smit, F., Toet, J., and van der Heijden, P. (1997). "Estimating the Number of Opiate Users in Rotterdam Using Statistical Models for Incomplete Count Data In European Monitoring Centre for Drugs and Drug Addiction (EMCDDA), 1997 Methodological Pilot Study of Local Prevalence Estimates. EMCDDA, Lisbon.

Smith, R. G. (2008). "Coordinating Individual and Organizational Responses to Fraud." *Crime, Law and Social Change, 49*:379-396.

– – – . and Gregor Urbas. (2001). "Controlling Fraud on the Internet: A CAPA Perspective: Report for the Confederation of Asian and Pacific Accountants, Research and Public Policy Series No. 39." Canberra: Australian Institute of Criminology.

Spam Act 2003. Act No. 129 of 2003, as amended.

Spiekermann, S., Grossklags, J., and Berendt, B. (2002). "E-privacy in 2nd Generation E-Commerce: Privacy Preferences Versus Actual Behavior," Proceedings of the Third AMC Conference on Electronic Commerce, 38-47.

Stroik, A. and Huang, W., (2009). "Nature and Distribution of Phishing," in Crimes of the Internet. Edited by Frank Schmalleger and Michael Pittaro. Upper Saddle River, NJ: Pearson Education Inc.

Symantec, (2010). "Symantec Global Internet Security Threat Report": Trends for 2009. Mountain View, CA: Symantec Corporation.

– – – .(2009). "Symantec Report on Rogue Security Software": July 08-June 09. Mountain View, CA: Symantec Corporation.

– – – .(2008). "Symantec Report on the Underground Economy": July 07-June 08. Mountain View, CA: Symantec Corporation.

Taylor-Butts, A., and Perreault, S. (2008). "Fraud Against Businesses in Canada: Results from a National Survey," Ottawa: Statistics Canada.

The Computer Fraud and Abuse Act of 1986, 18 U.S.C. § 1030.

The Council of Europe's *Convention on Cybercrime*, Budapest, 23.X1.2001, available online at: http://conventions. Coe.int/Treaty.en.Treaties/HTM/185.htm.

The Fair and Accurate Credit Transactions Act of 2003, Pub.L. 108-159.

*The Fair Credit Reporting Act***,** 15 U.S.C. § 1681 et seq.

The Fraud Act 2006 (2006 c.35).

United Kingdom. (2010). Home Office. "Cyber Crime Strategy." Norwich, UK: The Stationary Office.

United Nations Office on Drugs and Crime (UNDOC). (2010). "The Globalization of Crime": A Transnational Organized Crime Threat Assessment. Vienna: United Nations Office on Drugs and Crime.

United States Code, Title 18, §1029 (Access Device Fraud).

Urbas, G. and Choo, K.K.R. (2008). "Resource Materials on Technology-Enabled Crime: Technical and Background Paper No.28." Canberra: Australian Institute of Criminology.

van der Heijden, P., Cruyff, M., and van Houwelingen H., (2003). Estimating the Size of a Criminal Population from Police Records Using the Truncated Poisson Regression Model. *Statistica Neerlandica*, *57*:289–304.

Wagner, C. G. "Internet Fraud on the Rise." *The Futurist*, July-August, 2009.

Wall, D. S. (2010a)."Micro-Frauds: Virtual Robberies, Stings and Scams in the Information Age," in Corporate Hacking and Technology Driven Crime: Social Dynamics and Implications. T. Holt, B. Schell, eds., pp. 68-85, Hershey, PA: IGI Global.

– – – . (2010b). "Organizational Security and the Insider Threat: Malicious, Negligent and Well-Meaning Insiders." Mountain View, CA: Symantec Corporation.

– – – . (2009). "The Organization of Cybercrime and Organized Crime." A paper given to the Centre for Excellence in Police Studies, Australian National University, Canberra, Australia, April 28, 2009.

Walther, J. (2004). "Meeting the Challenge of Automated Patch Management." Bethesda, Maryland: SANS Institute.

Weaver, R. and Collins, M.P. (2007). "Fishing for Phishes: Applying Capture-Recapture Methods to Estimate Phishing Populations," APWG eCrime Researcher Summit, October 4-5, 2007, Pittsburgh, PA, USA.

Wennekes, K. (2008). "A Report of Canadian Executive and Frontline IT Security Professionals on Their Information Sources, Security Challenges, and Career Advantages." Ottawa: CATAAlliance.

White, M. D. and Fisher, C. (2008). Assessing Our Knowledge of Identity Theft: The Challenges to Effective Prevention and Control Efforts. *Criminal Justice Policy Review*, 19(1):3-24.

Zambo, S. (2007). “Digital La Costa Nostra: The Computer Fraud and Abuse Act’s Failure to Punish and Deter Organized Crime.” *New England Journal on Crime and Civil Confinement, 33*:551-575.