

Student and Non-Student Perceptions and Awareness of Identity Theft

John Winterdyk and Nikki Thompson

Department of Justice Studies, Mount Royal College

Dans plusieurs rapports récents, on a reconnu que l'usurpation d'identité est devenue une source importante de préoccupation pour les autorités policières et le système judiciaire au Canada. Même s'il y a une quantité considérable d'information descriptive sur l'usurpation d'identité et la fraude liée à l'identité au Canada, il y a peu de renseignements quant à la connaissance et la sensibilisation des gens sur le vol d'identité et le risque potentiel d'en devenir la victime. Dans cette étude, on a mesuré le niveau de perception et de sensibilisation de 360 collégiens ou universitaires et de 106 non-étudiants à la nature, à la portée, aux risques et aux effets de l'usurpation d'identité et d'une variété de comportements frauduleux, à l'aide d'une échelle d'auto-évaluation de Likert à 5 niveaux. Les résultats indiquent que les étudiants pourraient être sensiblement plus à risque, mais aussi mieux informés que les adultes non étudiants. À partir de ces données, certaines incidences sur les politiques générales et certaines stratégies de sensibilisation sont proposées, afin de mieux combattre ce problème au Canada. On suggère aussi quelques pistes de recherches éventuelles.

Mots clés : usurpation d'identité, perception du public, perception des étudiants, recherche-sondage, incidence politique

Several recent reports have recognized identity theft as a major concern to law-enforcement agencies and the judicial system in Canada. While there is considerable descriptive information on identity theft and identity fraud in Canada, there is a dearth of information about peoples' knowledge and awareness of identity theft and their potential risk to becoming a victim. This study measured the self-reported perception and awareness about the nature, extent, risk, and effects of identity theft and a variety of fraudulent behaviours among 360 college/university students and 106 non-students using a 5-point Likert scale survey. The findings indicate that students are perhaps slightly more at risk but are also somewhat better informed than adult non-students about identity theft. Based on the findings, some general policy implications and educational strategies are offered to better combat identity theft in Canada. A number of suggestions for future research are also proposed.

Keywords: identity theft, public perception, student perception, survey research, policy implications

Introduction

“I feel completely violated”—this phrase is commonly heard from those who have experienced identity theft and then had their personal information used to commit a fraudulent act. Why? Our identity is something that we all value. We are given a name at birth, we are assigned a Social Insurance Number (SIN), and we can readily obtain credit cards and bank cards. We are given a birth certificate with personal identifiers on it, and we have various forms of identification that contain our facial images (e.g., photo identification on our driver’s licences, passports, and even student ID cards).¹ It is virtually impossible to engage in any social interactions without disclosing, at some level, some degree of who and/or what we are.

One telephone survey of 1,005 adult Canadians, conducted by Environics Research Group, found that almost 6 in 10 Canadians carry their SIN card, even though 81% of the respondents felt that losing their SIN card would put them at the greatest risk for identity theft (MasterCard 2006). The survey also found that most Canadians believe that losing their driver’s licence or a credit card would put them at considerable risk as well (78% and 77% respectively).²

As noted on the website of the Office of the Privacy Commissioner of Canada, “Every year, thousands of people are victims of identity theft.” Security breaches of both privately and publicly held databases that hold our personal information is increasingly common. The recent security breach of the “Winners” and “HomeSense” retail chains are just one example. One estimate is that “thousands of Canadian credit-card holders have been victimized by fraud after a security meltdown” at Winners in which their personal information was “stolen” and then used to commit fraudulent acts (Stewart 2007: A1). Credit and debit-card security breaches are not the only source of identity theft, as we now know that medical, personal insurance, and employment databases have also been targeted. Yet, according to Cherry and Legatos (2006), until we have been a victim of identity theft, most of us do not fully realize the possible financial and personal implications and consequences. Cherry’s (2005) report indicates that more than 11,200 Canadians were victims of identity theft in 2005. In the same article, a crime-prevention officer notes that it can take up

Table 1: Number of identity theft articles by year¹⁸

Year	Number of News Articles
2006	1203
2005	1182
2004	880
2003	791
2002	298
2001	126
2000	71
1999	58
1998	3
1997	21
1996	1
1995	1
1994	0

to four years to get one's affairs back in order, depending on how diligent people are in documenting the tracking of precautions they have taken to protect their identities. Although not based on scientific research, such anecdotal observations serve as useful insights worthy of closer scrutiny.

There is a growing body of academic and non-academic information on identity theft. A search of Canadian Newsstand through the ProQuest search engine for the term *identity theft* revealed that since 2000 there has been a marked increase in the number of articles that included some type of coverage of identity theft (see Table 1). A similar search of Canadian Business and Current Affairs (CBCA) Business produced a list of 533 documents for identity theft from 2002 to 2006 with a trend similar to that found among the newspapers.

Although much of the research on identity theft is limited to data from the United States, some Canadian research is emerging. Typically, the Canadian literature tends to focus more on strategies individuals can take to protect themselves, while the American research tends to offer more insight on what strategies are being used by law-enforcement agencies to detect and prevent identity theft. The majority of research on identity theft focuses on four key areas: the amount and financial impact of identity theft, techniques being used to perpetrate identity theft, groups at greatest risk of being victims of identity theft, and law-enforcement strategies to detect and prevent identity theft.

Amount of identity theft and its financial impact

Academic and business-related sources have noted that identity theft is on the rise in North America and represents a significant concern to law-enforcement agencies (Chua 2003; Henderson 2005; Mayer 2005; Saffran 2005; U.S. Department of Justice 2005; Ward 2005).

In 2006, PhoneBusters, which collects information on ID theft and other forms of fraud in Canada, reported that there were 7,778 victims of identity theft (Perkins 2007). This figure is down noticeably from the 12,409 incidents in 2006 and the 11,938 incidents in 2005.³ Yet the value of reported loss for 2006 was significantly greater, at \$16.2 million versus \$8.6 million in value of reported loss in 2005. In addition, a 2005 telephone poll conducted by Ipsos Reid found that nearly 9%, or 2.7 million Canadians, have been victims of some type of identity theft at some point in their lives (Consumer Measures Committee 2005). In addition, 80% of the respondents said they consider identity theft to be a serious problem in Canada (38% a "very serious problem," 42% a "somewhat serious problem"). In 2006, the Royal Bank reported that in Canada alone there were in excess of 2 billion fraudulent credit card and debit card transactions in 2005 (Moneris Solutions...2006). Fraudulent business transactions made using credit cards and Internet shopping sites such as eBay, Plusone, Shoptoit.ca, and so on, have been growing at an ever-increasing rate.

Henderson (2005) reports identity theft as the fastest growing crime in North America, costing businesses millions of dollars each year. The *Economist* made a similar observation when it said identity theft is "one of the fastest growing white-collar crimes in the United States" (cited in Milne 2003: 391). The American Federal Trade Commission reported that in 2005, identity theft represented the most common complaint for the sixth straight year. A recent American survey found that 3% of the households in the United States had at "least one member of the household who had been the victim of identity theft during the previous 6 months" (Baum 2006: 8). Another American report by Consumer Sentinel, a complaint database maintained by the Federal Trade Commission (FTC), in 2005 reported that 37% of all complaints involved identity theft and that the age-group 18-29 accounted for the highest proportion of identity theft complaints by victims (29%) (FTC 2005).⁴

The problem of identity theft and related fraud is a growing global concern. Most are familiar with financial fraud scams such as the West

African fraud letters (WAFL) and the “Nigerian scam” (also known as 419 fraud) (Criminal Intelligence Service Canada 2007; Gaudin 2005). In addition, terrorists use identity theft as a source of funding their terrorist operations (Dart 2005; Hoar 2001; O’Brien 2004),⁵ and a Canadian study reported that identity fraud has been an integral part of smuggling undocumented migrants (Ronderos 2000).⁶ The growing diversity in the forms and methods of identity is not unique to North America. For example, a study on identity theft in the United Kingdom reported that organized crime has become heavily involved in identity-theft schemes because of the immense profits to be made and the difficulty in detecting and apprehending offenders because ID thieves are operating under the cover of another person’s identity (Cabinet Office 2002). The Home Office of London estimates that more than 100,000 people are victims of identity theft in the United Kingdom each year, costing the economy over 1.7 billion pounds annually (approximately CAN\$3.5 billion) (Home Office Steering Committee 2006). According to VAonline.org, five agencies are dedicated to assisting and addressing identity theft and identity fraud in the United Kingdom. This compares to eight in Canada, and seventeen in the United States, and only one for all of Continental Europe—the European Anti-Fraud Office (Victim Assistance Online 2007).

Forms and methods of identity theft

Academic sources (see Allison, Schuck, and Lersch 2005; Higgins, Hughes, Ricketts, and Fell 2005; Milne 2003; Ronderos 2000; Towle 2004) and governmental agencies (see online information posted by Public Safety and Emergency Preparedness Canada) categorize identity theft into four basic types. A further distinction is commonly made between the primary methods of identity theft (e.g., physical or electronic).

The most common form of identity theft occurs when offenders wrongfully obtain—usually through such physical means as “borrowing” or stealing other people’s identification information—to falsely misrepresent themselves when they are encountered by an authority. As Higgins et al. (2005: 165) note, this “type of fraud is a ‘true’ misrepresentation regarding the stopped person’s real identity.” Students might use this method when underage and trying to gain entry into a bar. A more serious misrepresentation might involve the use of another’s identity in order to avoid detection when dealing with the police or some other aspect of the criminal justice system.

A second form of identity theft involves using another person's identifying information in order to illegally establish a new bank/financial account in that person's name. The theft of one's identity can be obtained through both physical and/or electronic means. The theft is often the result of the offender obtaining relevant personal details from people through electronic techniques known as "spear phishing emails," "spoofing," "carding," or "phishing."⁷ Common physical methods of obtaining information include "shoulder surfing" (standing nearby and watching as the victim enters his or her PIN and password, or provides personal details to a clerk, etc.), and "dumpster diving" (rummaging through garbage in dumpsters or garbage bins to obtain discarded personal information). Lombardi (2006) reports that phishing is a rapidly growing form of identity theft, accounting for about 20–25% of such incidents. According to the 2006 *Consumer Reports State of the Net*, phishing scams cost American consumers an average of \$850 per incident, with total damages amounting to some US\$630 million and affecting 1 in 115 people (State of the Net 2006 2007).

A third illegal use of another person's identity is based on incidents that include a takeover or "hijacking" of another person's existing account. In such cases, the offender impersonates a victim in order to use her or his account to obtain something under false pretences. An electronic version of this technique might involve obtaining access to an unwitting victim's computer through clandestine methods (Towle 2004). While anti-virus and anti-spam software is helpful in reducing the risk of having one's personal or sensitive information stolen, there is always a risk of such information being accessed whenever one is online (Lombardi 2006; Slitz 2004). Similar forms of victimization can occur through other physical methods, provided the offender is able to access personal information through fraudulent means, such as corruption or creating fraudulent statements.

The fourth category of identity theft involves the creation of a fictitious identity using the information of either a deceased person (i.e., genuine information) or other surreptitious means (i.e., invented). For example, mail might be stolen or diverted, personal information might be stolen from one's home, or information might be scammed through email in which the fraudster poses as a legitimate company or government agency in order to fraudulently obtain personal details that can then be used to create a new false identity. Another form of this technique can occur when the offender assumes the identity

of a deceased individual, then uses the identification to engage in fraudulent acts (Hoar 2001). Such actions are becoming more common among organized crime factions that are engaged in the manufacture and distribution of illegal drugs such as "crystal meth" and crack cocaine (see Ronderos 2000). Prior to 2002, there were no regulatory chemical controls in Canada. This freedom allowed drug traffickers who used fictitious identities to purchase explosives precursors and other chemicals frequently used in the clandestine production of controlled substances (Cabinet Office 2002). Another emerging trend in North America is the use of created identities by undocumented immigrants looking to establish a "legal" identity in order to live and work in a new country.⁸

In summary, the manner by which criminals instigate identity theft and related fraud is diverse and growing more sophisticated. This includes such techniques as online scams (e.g., fake e-commerce sites, auction fraud, and job offer scams), telephone-based scams (e.g., telemarketing fraud and 900 scams); fraudulent printed material (e.g., bogus lottery-winning letters that are sent out via mail with the receiver's correct address and name), and other acts (e.g., theft or loss of personal information and misrepresented personal data collection) (RCMP 2006). This range of techniques makes efforts to detect and prevent identity theft ever more challenging for law-enforcement and related agencies and organizations.

We are not only a consumer-oriented society but also one in which we increasingly make purchases with credit, debit, and gift cards. Given the often electronic nature of identity theft, it comes as no surprise that the risk of identity theft and related forms of fraud appear to be growing in frequency and level of sophistication (U.S. Department of Justice 2005). Yet in spite of the increased risk of having one's identity stolen or used, people tend to have little tolerance for security measures to protect their personal information. While most people do not mind using PINs, passwords, and/or other key devices like a smart card to protect their identities, Lombardi (2006) points out that sometimes such preventative measures are simply not sufficient to deter potential offenders. Biometric identification technology, while generally reserved for high-security matters, is considered to be intrusive, excessive, and more costly than conventional, less successful measures of protection (Frank 2004). Yet, as Huopio (1998) notes, biometric identification methods tend to be significantly better than the measures commonly used today.⁹ As biometric techniques become more

widely available, we are likely to see more Canadians and Canadian organizations using this type of technology to reduce their risk of being a victim of identity theft.¹⁰

Groups at risk of identity theft

Using 2002 data from the Federal Trade Commission in the United States, the Economic Crime Institute at Utica College reported that people between the ages of 30 and 39 accounted for 28% of reported identity theft victims, while those between the ages of 18 and 29 accounted for 26% of the reported identity theft victims (those under the age 18 accounted for just 2%) (Gordon, Willox, Rebovich, Regan, and Gordon 2004). Using data from the Identity Theft Resources Centre in the United States, Walters (2006) reports that post-secondary educational institutions "were more than twice as likely to report suffering a breach as any other type of entity."¹¹ Walters also found that security breaches by hackers created the largest number of potential victims. Furthermore, Shamlian (2005) found that the elderly and young adults are frequently victimized by those known to them, including family and friends who have access to their personal information.

While there is little information on the perceptions and awareness that college/university students have about identity theft, considerable research has been done with this group related to views on a range of crime and justice-related topics. This research includes general attitudes towards crime and justice (Bureau of Justice Statistics 2007), correctional policies (Bohm 1990; Hensley, Miller, Tewksbury, and Koscheski 2003; Miller, Tewksbury, and Hensley 2004; Mackey and Courtright 2000), and drug/gambling-use policies (Giacopassi, Vandiver, and Stitt 1997; Perkins, Meilman, Leichter, Cushin, and Presley 1999; Sullivan 1997). As well, college/university students have been surveyed on police and policing issues (Brown and Benedict 2005; Mesko, Umek, and Musek 1996), fear of crime and/or perceptions of personal safety (Istitute of Education Sciences 2005; Robinson 1999), and perception of young offenders (Peterson-Badali and Koegl 1996).

A review of the literature showed a lack of studies on the perception held by college/university students about identity theft. Only two studies were found (Higgins et al. 2005; Milne 2003), both based in the United States. Drawing on a sample of 61 college students and 59 non-students, Milne found that "consumer education seems to

be wanting for these two consumer sample groups" (399). Higgins et al., drawing on a sample of 243 students, concluded "that [American] college students do not have a solid grasp of identity theft" (16), even though they fall within the most often victimized age group for identity theft and identity fraud.

The law and related countermeasures

Unlike in the United States where there are state and federal laws to address the problem of identity theft (see Gordon et al. 2004; Higgins et al. 2005; Hoar 2001; Milne 2003), the Criminal Code of Canada does not outline a single and separate offence for identity theft. Instead, the Canadian Criminal Code outlines 30 different relative offences. These include:

- Personation (section 403)
- Forgery of or uttering forged passport (sections 57, 58)
- Forging, use, and trafficking of forged or falsified credit cards (section 342)
- Interception of any function of a computer system (section 342.1)
- Possession of device to obtain computer service (section 342.2)
- Forging and uttering forged document (section 366)
- Conspiracy (section 465 (1) (c)).

While provincial legislation related to identity theft is currently limited, most provinces are developing programs to raise awareness. Government and consumer groups are now providing tools and strategies to combat identity theft. In 2004, Ontario became the first province to embark on an information campaign to raise public awareness of identity theft and provide tips on how to protect consumers from becoming victims (see, for example, Ministry of Government and Consumer Services 2008). However, while "information practices mandated by existing laws already require breach notification under certain circumstances," only Ontario's Personal Health Information Protection Act of 2004 includes explicit provisions to protect people whose personal health information has been breached by requiring victim notification (Canadian Internet Policy and Public Interest Clinic [CIPPIC] 2007: 2). British Columbia's Office of the Information and Privacy Commissioner (OIPC) is working with police agencies, government agencies, and other groups to address the growing problem of identity theft on a number of formal and informal levels. Similar efforts have been initiated by Alberta and Quebec (CIPPIC).

In addition to the legislative changes and a network of statutory and common law privacy laws in Canada, a growing number of Internet sites (e.g., Public Safety 2008) offer information and educational tips on how to protect one's identity. There are also software programs to protect against possible personal information theft on the Internet (e.g., GhostSurf Platinum 2007).¹²

As noted in the recent White Paper prepared by the Canadian Internet Policy and Public Interest Clinic, every business in Canada that handles customer information is governed by the federal Personal Information Protection and Electronic Documents Act (PIPEDA) "or its provincial equivalent in Alberta, British Columbia and Quebec" (CIPPIC 2007: 2). In accordance with these statutes, businesses are required to employ reasonable security measures to protect personal information. The act also provides for mandatory notification of security breaches when certain types of personal information have been accessed without proper authority (see CIPPIC).¹³ As recently as 2005 (see Henderson 2005) no provinces in Canada had breach-notification legislation that required victims to be told when their personal information had been leaked or stolen from a private business. However, in 2006 the British Columbia and Ontario privacy commissioners produced a four-page document that outlined when an organization needs to notify individuals of a breach (CIPPIC).¹⁴

While a growing number of the provinces have or are developing related legal provisions, a number of resources are available for contacting and reporting and detecting identity theft. For example, PhoneBusters, operated jointly by the Ontario Provincial Police and the RCMP, serves as an anti-fraud call centre and collects and disseminates related information. Other services include Internet Scambusters, Reporting Economic Crime Online, Equifax, and TransUnion (for reporting credit card and fraud alerts), the privacy commissioner of Canada, and the Canadian Bankers Association. In addition, a wide range of non-profit organizations also provide services to potential identity-theft victims, including the Identity Theft Resource Center, BBBOnline, and the Credit Union National Association (see Public safety 2008).

Most major businesses today offer countermeasure tips on how individual consumers can protect themselves. Common recommendations include sharing personal identity information only when

necessary; not carrying unnecessary identity information; not disclosing your personal PIN or similar type of identifier codes with others; regularly changing your PIN; cleaning out your garbage and recycling documents from your computer; routinely reviewing all your financial statements; and periodically requesting copies of credit reports (O'Brien 2004). Victims of identity theft should contact the security or fraud departments for any creditors, file a report with the local police department, close existing accounts (e.g., bank, credit union, credit card companies), and change PINs and passwords (see Hoar 2001 for further details).

Void in research

While research on fraud has a long tradition (see, for example, Brennan 1999; Lemert 1953; McPhie 1996; Trembley 1986), little has been done on identity theft. As noted in Allison et al. (2005), Higgins et al. (2005), Milne (2003), and Towle (2004), more research needs to be undertaken to document the extent of the different types of identity theft. More research is also needed to detail the losses to society as identity theft grows and takes on different expressions.

While research demonstrates that identity theft is occurring at an ever-increasing rate, and that attempts are underway to inform the public, little research has been done to empirically measure public awareness. Only anecdotal information informs our understanding of a multitude of questions: Does the public have an accurate perception of the amount of identity theft in Canada? Are the public aware of the ways they can become victims of identity theft? How aware are the public on the ways they can prevent identity theft? And what actions do the public actually take to prevent identity theft?

Even though the United States has been more aggressive in implementing legislation to tackle and address offences related to identity theft, Higgins et al. (2005: 168) point out that these actions "do not provide direct insight into the actions of one highly susceptible target for identity theft and fraud—college students." The same observation would appear to apply equally to the Canadian situation, as there is a dearth of information about identity theft as it relates to Canadian college/university students.

Present study

This exploratory study adds to the limited body of empirical literature on the awareness and perception of identity theft in Canada. Specifically, we examine the general knowledge and perceptions about identity theft for one potentially vulnerable group—college/university students. Their responses will be compared to a group of non-students.

College/university students are used as the research population for several reasons. They are often more technologically savvy and experienced. As well, they are heavily courted as clients by financial institutions but may not be as knowledgeable about complex financial transactions. Last, according to victimization research, college/university students fall into the highest-risk age category for criminal victimization (see CCJS 2000; Higgins et al. 2005; Milne 2003).

This exploratory study aims to establish a better understanding of student and non-student differences regarding identity theft as well as their respective knowledge about fraudulent behaviours (e.g., bank fraud, credit card fraud, fraudulent loans, telecommunications fraud, and phone or utility fraud). As in the studies by Milne (2003) and Higgins et al. (2005), we are interested in learning about what measures, if any, either group takes to protect their identity and how they might differ. As well, we want to examine risk and self-protective behaviours that each group engages in throughout their daily lives. Also, this study will provide empirically supported information to assist post-secondary institutions and other agencies in developing procedures and policies that might help increase student awareness and reduce the risk of student victimization.

Operational definition of identity theft

For the purpose of this study, we use a general definition of identity theft provided by the RCMP: Identity theft involves stealing, misrepresenting or hijacking the identity of another person or business and provides an effective means to commit other crimes (RCMP 2007). This is the same general definition supported by research conducted by the Ponemon Institute, a research think-tank based in Elk Rapids, MI (Lombardi 2006). Similar definitions are used by such major organizations and institutions as the Privacy Commissioner of Canada, Canadian Bankers Association, and the Canadian Chamber of Commerce.

Methods

The study group

Survey data for the students and non-students were collected during the spring of 2006. Using research protocols from the U.S. studies conducted by Higgins et al. (2005) and Milne (2003), a survey was drafted in both print and in electronic/online (e.g., SurveyMonkey) form. The paper version was pilot-tested with several different student groups as well as with members of the public. The online version was pilot-tested by requesting that it be completed by people known to the research assistants and principal researchers. Ten people completed the paper version while 7 completed the online version. As a result of the pilot test, a few minor revisions were made to the survey.

The survey and research proposal were presented to the school's Research Ethics Committee for review. Following its approval, two upper-level undergraduate students from our department were hired to administer the survey as well as to enter the data using the Statistical Package for the Social Sciences (SPSS).

The research assistants were instructed to survey a cross-section of full-time registered students across all the major disciplines at the school. They employed a snowball sampling method to identify prospective instructors and classes to ensure the desired sample size ($N = 400$).

The non-student group was surveyed by the research assistants through convenience sampling (by contacts they had in the community), as well as a snowball sampling approach. If members of the public did not have time to complete the survey with the research assistant, they were given a website address to fill out the survey online at their convenience.¹⁵ A total of 106 surveys were completed.

All participants were provided with either written or oral instructions on the purpose of the study and a guarantee that participation was both anonymous and confidential. There was a draw prize (an MP3 player) available to anyone who participated. To qualify for this draw, participants could submit contact information on a separate piece of paper via the survey's website.

Of the 400 students sampled, 360 (80%) surveys were completed. The non-student sample was 106. The average age of the student

sample was 24 years, and 36 years for the non-student group. The student age range was 18–55 years, and 20–75 years for the non-student group.¹⁶ The entire sample, including students and non-students, consisted of 197 males and 269 females, with 76.2% of Caucasian descent, and 23.8% of non-Caucasian decent.

Measures

The survey instrument comprised seven sections. Respondents were asked to indicate their level of knowledge about five primary types of fraud (credit card fraud, telecommunications fraud, phone or utility fraud, bank fraud, and fraudulent loans) using a 5-point Likert scale ranging from “very little knowledge” (1) to “a great deal of knowledge” (5).

In addition to questions of general knowledge about identity theft, respondents were asked to complete a series of questions on the steps they might take to protect themselves from identity theft; how often respondents engaged in activities that increased their likelihood of being victimized (e.g., making purchases through the Internet; using their credit/debit card to make purchases, on a scale ranging from “1–3 times” up to “13 or more times”); and their perceptions of the incidence of various types of identity theft (from 0% to 100%). The final section of the survey consisted of six questions that asked respondents who had been a victim of identity theft in the past year to provide detail about the impact and outcome of the event.¹⁷

Results

The results of the survey of non-students and students can be divided into four categories: knowledge of identity theft, participation in financial transaction, perception of identity as a problem, and perception of identity-theft reporting.

Knowledge of identity theft

The first section of results report on the level of knowledge students believed they have about five forms of fraud that could be the result of identity theft: credit card fraud, telecommunications fraud, phone or utility fraud, bank fraud, and fraudulent loans. As seen in Table 2, neither students nor non-students indicated they knew little about any of the types of fraud. However, statistically significant relationships were found between a person’s status (student or non-student) and

Table 2: Student and non-student knowledge of identity theft

How much do you know about:	Very Little		A Little		Some		A Lot		A Great Deal		r_s & Sig.
	NS ^a	S ^b	NS	S	NS	S	NS	S	NS	S	
Credit card fraud	8.5% (N = 9)	10.9% (N = 39)	17.9% (N = 19)	26.5% (N = 95)	46.2% (N = 49)	45.5% (N = 163)	21.7% (N = 23)	13.9% (N = 50)	5.7% (N = 6)	3.3% (N = 12)	$r_s = -.117^c$
Telecommunications fraud	31.4% (N = 33)	39.3% (N = 141)	32.4% (N = 34)	33.4% (N = 120)	24.8% (N = 26)	18.9% (N = 68)	9.5% (N = 10)	7.0% (N = 25)	1.9% (N = 2)	1.4% (N = 5)	$r_s = -.085$
Phone or utility fraud	42.5% (N = 45)	59.8% (N = 213)	24.5% (N = 26)	22.5% (N = 80)	22.6% (N = 24)	15.4% (N = 55)	10.4% (N = 11)	1.4% (N = 5)	0.0% (N = 0)	0.8% (N = 3)	$r_s = -.17^d$
Bank fraud	19.8% (N = 21)	25.9% (N = 92)	30.2% (N = 32)	27.3% (N = 97)	34.0% (N = 36)	30.1% (N = 107)	13.2% (N = 14)	12.4% (N = 44)	2.8% (N = 3)	4.2% (N = 15)	$r_s = -.035$
Fraudulent loans	33.3% (N = 35)	47.3% (N = 169)	32.4% (N = 34)	28% (N = 100)	21.0% (N = 22)	17.1% (N = 61)	8.6% (N = 9)	5.9% (N = 21)	4.8% (N = 5)	1.7% (N = 6)	$r_s = -.127^d$

^a Non-student

^b Student

^c Significant r_s at a $p < .05$.

^d Significant r_s at a $p < .01$.

Bold indicates most frequent response.

Table 3: Student and non-student purchasing overview

In an average month, how many times did you:	1–3 Times		4–6 Times		7–9 Times		10–12 Times		13 or More Times		r_s & Sig.
	NS ^a	S ^b	NS	S	NS	S	NS	S	NS	S	
Purchase something off the Internet?	72.9% (N = 70)	91.2% (N = 237)	20.8% (N = 20)	5.8% (N = 15)	5.2% (N = 5)	1.9% (N = 5)	1.0% (N = 1)	0.8% (N = 2)	0.0% (N = 0)	0.4% (N = 1)	$r_s = -.230^c$
Use debit cards to purchase items at a store?	21.2% (N = 22)	99% (N = 35)	23.1% (N = 24)	11.9% (N = 42)	12.5% (N = 13)	13.4% (N = 47)	12.5% (N = 13)	199% (N = 70)	30.8% (N = 32)	44.9% (N = 158)	$r_s = .185^c$
Use your credit cards?	67.3% (N = 66)	81.9% (N = 227)	20.4% (N = 20)	11.2% (N = 31)	10.2% (N = 10)	3.6% (N = 10)	1.0% (N = 1)	0.7% (N = 2)	1.0% (N = 1)	2.5% (N = 7)	$r_s = -.166^c$
Use personal checks to purchase items at a store?	67.3% (N = 66)	81.9% (N = 227)	20.4% (N = 20)	11.2% (N = 31)	10.2% (N = 10)	3.6% (N = 10)	1.0% (N = 1)	0.7% (N = 2)	1.0% (N = 1)	2.5% (N = 7)	$r_s = -.435^c$

^a Non-student

^b Student

^c Significant r_s at a $p < .01$.

Bold indicates most frequent response.

Table 4: Student and non-student estimation of identity theft problems

In the past 12 months, have you thought that any of the below are problems where you live/work?	To a Very Small Extent		To a Small Extent		To Some Extent		To a Great Extent		To a Very Great Extent		r_s & Sig.
	NS ^a	S ^b	NS	S	NS	S	NS	S	NS	S	
Credit card fraud	35.2% (N = 37)	47.2% (N = 167)	22.9% (N = 24)	20.3% (N = 72)	27.6% (N = 29)	20.3% (N = 72)	10.5% (N = 11)	8.8% (N = 31)	3.8% (N = 4)	3.4% (N = 12)	$r_s = -.097^c$
Telecommunications fraud	53.3% (N = 56)	68.8% (N = 240)	24.8% (N = 26)	17.8% (N = 62)	17.1% (N = 18)	9.7% (N = 34)	3.8% (N = 4)	1.7% (N = 6)	1.0% (N = 1)	2.0% (N = 7)	$r_s = -.136^d$
Phone or utility fraud	56.2% (N = 59)	75.7% (N = 262)	24.8% (N = 26)	15.0% (N = 52)	17.1% (N = 18)	6.9% (N = 24)	1.0% (N = 1)	2.3% (N = 8)	1.0% (N = 1)	0.0% (N = 0)	$r_s = -.18^d$
Bank fraud	45.7% (N = 48)	64.2% (N = 224)	27.6% (N = 29)	15.8% (N = 55)	16.2% (N = 17)	12.0% (N = 42)	9.5% (N = 10)	5.7% (N = 20)	1.0% (N = 1)	2.3% (N = 8)	$r_s = -.140^d$
Fraudulent loans	56.2% (N = 59)	76.7% (N = 264)	24.8% (N = 26)	12.8% (N = 44)	12.4% (N = 13)	8.4% (N = 29)	5.7% (N = 6)	1.5% (N = 5)	1.0% (N = 1)	0.6% (N = 2)	$r_s = -.192^d$

^a Non-student

^b Student

^c Significant r_s at a $p < .05$.

^d Significant r_s at a $p < .01$.

Bold indicates most frequent response.

three forms of fraud: credit card fraud ($r_2 = -.117, p < .05$), utility fraud ($r_2 = -.174, p < .01$), and fraudulent loans ($r_2 = -.127, p < .01$).

Overall, students seemed less well-informed about credit card fraud (the stealing and/or illegal use of another person's credit card or credit card number), phone or utility fraud (the illegal use of another person's phone service or electricity by a wide range of methods, including "slamming," PBX phone scam, 809 phone scams, etc.), and fraudulent loans (the stealing of someone's personal information to obtain a loan in his or her name) than were the non-students.

Participation in financial transactions

The second section of the survey asked respondents to estimate the amount of time they spent in capacities such as engaging in online transactions and/or purchasing. Statistically significant relationships were found across all four dimensions of respondent purchasing activities each month, including Internet, debit, credit card, and checks. Response choices ranged from "1-3 times" a month to "13 or more times" a month for each activity choice.

It was found that students spend less time than non-students purchasing something on the Internet ($r_2 = -.230, p < .01$), using credit cards in a store ($r_2 = -.166, p < .01$), and using personal cheques in a store ($r_2 = -.435, p < .01$). However, a relationship was found between the number of times respondents use their debit card in a store ($r_2 = .185, p < .01$), indicating that even though students use fewer cheques, have fewer credit card transactions, and engage less often in online shopping, they are more likely to use more debit transactions when shopping in stores.

Perception of identity theft as a problem

The third part of the survey used a 5-point Likert scale ranging from "to a very small extent" to "to a great deal." This section asked respondents if they thought any of the five types of fraud covered in the survey posed a problem where they live or work. In both groups, the primary response was "to a very small extent." In the case of credit card fraud, both groups said it was a problem "to a small extent." It was found that a statistically significant but weak relationship existed among all five categories of identity theft ($p < .05$). On average, the non-student group thought it was a problem "to a small extent," while on average the student group reported it was a problem "to a very small extent."

Table 5: Student and non-student estimates on forms of identity theft

Estimates of Identity Theft	Non-Student Mean Estimates	Student Mean Estimates	Mean Difference & Sig.
12. Please estimate the percentage of identity theft victims that reported unauthorized credit card charges were made in their name.	32.16% SD = 24.8	43.20% SD = 26.6	11.043**
13. Please estimate the percentage of identity theft victims that reported a credit card was opened in their name.	23.93% SD = 21.6	31.60% SD = 24.7	7.662**
14. Please estimate the percentage of identity theft victims that reported that the identity thief had established a new telephone in their home in their name or accessed their existing account.	16.43% SD = 19.0	25.07% SD = 22.0	8.638**
15. Please estimate the percentage of identity theft victims that reported that the identity thief had established a new cellular phone in their name or accessed their existing account.	18.49% SD = 20.3	29.11% SD = 23.8	10.613**
16. Please estimate the percentage of identity theft victims that reported the identity thief had established a new utility service in their name or accessed their existing account.	14.51% SD = 19.0	23.92% SD = 21.2	9.419**
17. Please estimate the percentage of identity theft victims that reported the identity thief opened a new bank account in their name.	14.52% SD = 20	26.80% SD = 24.6	12.277**
18. Please estimate the percentage of identity theft victims that reported the identity thief wrote fraudulent checks in their name.	22.17% SD = 22.2	34.68% SD = 26.6	12.515**
19. Please estimate the percentage of identity theft victims that reported the identity thief obtained a loan (e.g., personal, business, auto, real estate, etc.) in their name.	16.70% SD = 20.9	27.09% SD = 24.7	10.383**
20. Please estimate the percentage of identity theft victims that reported the identity thief used their personal information to obtain employment.	12.64% SD = 19.6	24% SD = 23.9	11.365**

** Indicates r_s at a $p < .01$.

Note: Actual figures for each category are not available in Canada, as a result of variations in reporting and collecting methods between agencies. However, as based on conversations and data provided by PhoneBusters, these estimates seem somewhat high. As discussed under "The lure of money," there is no single agency that collects all fraud victim information.

Perception of identity theft reporting

In the fourth section of the survey, respondents were asked to estimate the percentage of identity-theft victims they think reported the incident to authorities, in relation to the five types of identity theft covered

Table 6: Student and non-student protective behaviours

How Often Do You:	Never		A Few Times a Year		Once or Twice a Month		At Least Once a Week		Almost Every Day		r_s & Sig.
	NS ^a	S ^b	NS	S	NS	S	NS	S	NS	S	
Review your bank statements	2.8% (N = 3)	6.2% (N = 22)	12.3% (N = 13)	20.8% (N = 74)	35.8% (N = 38)	51.0% (N = 181)	31.1% (N = 33)	18.3% (N = 65)	17.9% (N = 19)	3.7% (N = 13)	$r_s = -.244^d$
Review your credit card statements	1.9% (N = 2)	14.3% (N = 48)	7.7% (N = 8)	10.4% (N = 35)	40.4% (N = 42)	53.7% (N = 180)	30.8% (N = 32)	17.6% (N = 59)	19.2% (N = 20)	3.9% (N = 13)	$r_s = -.290^d$
Make purchases over the Internet without solicitation	41.3% (N = 43)	58.4% (N = 199)	39.4% (N = 41)	29.6% (N = 101)	14.4% (N = 15)	9.4% (N = 32)	4.8% (N = 5)	2.1% (N = 7)	0.0% (N = 0)	0.6% (N = 2)	$r_s = -.147^d$
Make an Internet purchase based on an ad/solicitation	73.8% (N = 62)	85.5% (N = 236)	20.2% (N = 17)	12.0% (N = 33)	6.0% (N = 5)	2.2% (N = 6)	0.0% (N = 0)	0.4% (N = 1)	0.0% (N = 0)	0.0% (N = 0)	$r_s = -.133^c$
Give out personal information over the Internet when making a purchase	47.6% (N = 49)	49.6% (N = 172)	39.8% (N = 41)	39.8% (N = 138)	8.7% (N = 9)	9.5% (N = 33)	2.9% (N = 3)	1.2% (N = 4)	1.0% (N = 1)	0.0% (N = 0)	$r_s = -.025$
Make purchases over the phone	72.4% (N = 76)	76.4% (N = 268)	21.9% (N = 23)	19.9% (N = 70)	5.7% (N = 6)	3.1% (N = 11)	0.0% (N = 0)	0.3% (N = 1)	0.0% (N = 0)	0.3% (N = 1)	$r_s = -.042$
Give out personal information over the phone	51.0% (N = 53)	54.7% (N = 192)	41.3% (N = 43)	37.0% (N = 130)	6.7% (N = 7)	7.1% (N = 25)	1.0% (N = 1)	0.6% (N = 2)	0.0% (N = 0)	0.6% (N = 2)	$r_s = -.026$
Limit the amount of your personal information given	30.5% (N = 32)	14.0% (N = 48)	23.8% (N = 25)	27.8% (N = 95)	15.2% (N = 16)	20.8% (N = 71)	9.5% (N = 10)	12.9% (N = 44)	21.0% (N = 22)	24.6% (N = 84)	$r_s = .125^d$
Contact organizations that you deal with to limit security risks	43.8% (N = 46)	58.1% (N = 201)	33.3% (N = 35)	26.6% (N = 92)	12.4% (N = 13)	8.1% (N = 28)	5.7% (N = 6)	2.0% (N = 7)	4.8% (N = 5)	5.2% (N = 18)	$r_s = -.122^d$
Give out your Social Insurance Number	73.3% (N = 77)	50.4% (N = 179)	21.0% (N = 22)	46.2% (N = 164)	3.8% (N = 4)	2.0% (N = 7)	1.9% (N = 2)	0.8% (N = 3)	0.0% (N = 0)	0.6% (N = 2)	$r_s = .175^d$

^a Non-student

^b Student

^c Significant r_s at a $p < .05$.

^d Significant r_s at a $p < .01$.

Bold indicates most frequent response.

in this study. As shown in Table 5, students provided estimates that were significantly higher across all items.

Both the students and non-students surveyed estimated the typical age of identity theft victims to be between the ages of 31 and 39 years. The average age of identity theft-victims in Canada is not known. However, research from the United States indicates that the 18–20 age group accounts for the highest proportion of identity-theft complaints (29%) (Consumer Fraud . . . 2005).

Risky practices

The fifth section of the survey consisted of questions intended to obtain an informal sense of how careful respondents were in giving out their personal information in ways that increase their risk of victimization. These “risky” behaviours include providing personal information when making Internet purchases, giving out their SINs, making credit card purchases over the phone, and failing to review their bank and credit card statements. As seen in Table 6, students tend to review bank statements less, review credit card statements less, make purchases over the Internet with and without solicitation less, and contact organizations to deal with security risks less frequently than do the non-student group. A statistically significant relationship was also found between student and non-student status and the amount of personal information the respondents disclosed about themselves. For example, the student group tended to give out their personal information and their Social Insurance Number more often than did the non-students.

Interestingly, it was found that students tend to use secure websites more often to perform online secure transactions when compared to the non-student group ($r_2 = .219, p < .01$). However, students were less inclined to utilize a safety deposit box to secure personal information ($r_2 = -.212, p < .01$).

Respondents’ self-reported identity-theft victimization

The final section of the survey focused on details of the event in which the respondent was a victim. Only 6.4% ($N = 23$) of students had been a victim of identity theft, while 12.3% ($N = 13$) of the non-students/general public acknowledged being a victim of identity theft.

Of the 36 respondents who had been victimized, close to 100% of both student and non-student groups reported they had been victimized "1–3 times" in the past two years. Credit card fraud was the most common self-reported type of offence, with about 61% of both student and non-student victims reporting this type of victimization. It is difficult to make definitive statements about the frequency of other types of identity-theft victimization because the total number of respondents in each category was quite small. However, it was found that about 20% of student victimization was due to bank fraud, compared to about 8% of non-student victimization. Approximately 15% of non-student victims and 13% of student victims indicated they experienced other forms of fraud (e.g., vehicle loan, debit card fraud, video rental, and voting scandal). Neither group reported significant numbers of non-vehicle loan fraud, telecommunications fraud, or phone or utility fraud. Overall, the trend was slightly different from that reported by the Federal Trade Commission in their 2006 annual report, in which credit card fraud was the most common form of identity theft (26%), followed by phone or utility fraud (18%), and then bank fraud (17%) (MyTruston 2007).

Of those who reported having their identity stolen in the past two years, 23% of the non-students and 44% of the students indicated they noticed their victimization "within days." A significant number of student victims (35%) reported they realized their victimization "within minutes" or "within hours" of the incident, compared to only a few (15%) non-students. Approximately 62% of the non-student victims and 22% of the student victims indicated they first noticed their victimization only after several weeks or months had passed.

Those respondents who had been a victim of identity theft indicated that it is time-consuming to remedy the situation. Nearly 70% of the non-student group and 78% of the student group estimated that it took them between a "few hours" and a "few days" to resolve, noting they spent anywhere from a few hours to a few days in resolving the immediate consequences of their victimization. For some, it took longer. Close to 23% of the non-student victims and 17% of the student victims stated it took several weeks to months to rectify issues. A few respondents indicated they spent over a year dealing with the consequences of their victimization.

While several sources examined for this study indicated that most identity-theft victims pay financially to restore their identity, our study's findings suggest such costs were not significant. Close to half

of identity-theft victims in this study (46% of the non-student group and 52% of the student group) reported that it did not cost them anything to restore their identity. Of the non-student group, 30% reported it cost them \$1–\$299, and 15% reported costs of \$300–\$799. The group of student victims reported similar results; 26% spent \$1–\$299 to repair the damage and 17% spent \$300–\$799. Only 2 of the 36 (5.6%) victims indicated that it cost them more than \$800 to recover their identity.

Discussion

Consistent with the findings in Higgins et al. (2005), our respondents had some blind spots in their awareness of certain types of identity theft. While having some awareness of credit card theft and fraud, both the non-student and student groups were less knowledgeable about the other forms of identity theft (e.g., telecommunications fraud, phone or utility fraud, and fraudulent loans). Our results do not differ significantly from those of Higgins et al., who studied U.S. citizens. Because official Canadian statistics on the incidence of identity theft in its various forms are not collected, it is difficult to evaluate the accuracy of estimates of identity theft provided by respondents of this study. However, using official statistics on identity theft from the United States as a comparison, it appears that both the non-student and student groups in this study overestimate the actual occurrence of identity theft. Between the two groups, students believe identity theft is more common than non-students. This difference is inconsistent with the finding that students reported a lower incident of identity-theft victimization.

In general terms, the results of this study indicate that neither non-student nor student respondents are sufficiently aware of the issues related to identity theft. However, there are some differences between the two groups in specific areas of risk. Students tend to use debit cards more frequently than non-students, who in time are more likely to use credit cards and personal cheques. Perhaps as a result of their greater exposure to computers, students are more likely to use secure websites when making online purchases than non-students. They are also less likely to review their bank-account and credit-card statements. Students reported they gave out personal information such as their SIN more frequently than non-students. This exposes students to the potential of more identity-theft victimization.

Policy considerations and future research

Although the student and non-student samples were limited to a major Western Canadian city, a number of tentative policy considerations can be offered on the basis of results from this study. Any recommendations, however, should bear in mind Sproule's observations that "until such classifications are clarified, it is difficult for business, government, and the public to understand the level of activities and their impact on organizations and individuals, in making comparisons over time and among different jurisdictions" (DeGroot 2007).

Given that there was a difference in knowledge and perception between non-students and students, it would appear prudent that both groups be targeted for information and preventive strategies regarding identity theft. While the efforts of the RCMP are to be commended (see RCMP 2006), we would suggest, on the basis of our findings, that the protocol developed could be adapted for other age groups as well. Future studies should discern which types of lifestyle activities are related to risk of identity theft. This information could then be used to better identify what type of educational information would work best with different target populations.

In addition, on the basis of our findings and the growing concerns over identity theft, we support the views expressed in the White Paper (see CIPPC 2007) on modernizing Canadian criminal law and amending the PIPEDA, calling for an updating of legislation so that it can be more effectively used to combat identity theft. Consistent with a recommendation put forth by the Canadian Bankers Association (CBA), we also feel that the term *personal information* needs to be defined in the Criminal Code, and that an identity-theft prevention policy should be developed, based on factual evidence and one that embraces a multi-pronged approach. Such an approach could include, among other options, new laws and regulations, technology, education, training, strong leadership, and information policy needed to better address identity theft/fraud (see Gordon et al. 2004).

As with all successful crime prevention, educating people about the risk of identity theft, and developing strategies to combat it, requires an innovative and diverse approach. Given the students' general lack of knowledge and the misconceptions they hold about identity theft, colleges and universities need to consider providing specific

education and training programs about these issues as part of student orientation. On the basis of our findings, any educational initiative should not only be focused on specific areas but should also alert students to emerging trends.

Future research needs to examine why students and non-students not only differ in their understanding and perceptions, but also why they do not have a good grasp of the risk of identity theft and identity fraud, in spite of all the information available. However, as long as most Canadians value economic success and are prepared to carry several pieces of identification on their person, it will be difficult to develop social policies that will significantly reduce crimes of identity theft and related fraud. While certain target-hardening initiatives have been devised, criminals seem to be able to find new twists to the old snake oil formula.

Conclusion

The present study shows that college/university students are generally less well informed about identity theft and identity fraud than non-students. In purchasing habits and estimation of identity-theft risk, there were differences between the groups, with students expressing less concern about their potential risk of being victimized. Students were also somewhat less inclined to review their credit card statements, and exercised less caution when purchasing online. In general, students appeared somewhat more naïve about the problem and their risk of being a victim of identity theft or fraud. These general results are consistent with the findings of both Higgins et al. (2005) and Milne (2003).

Finally, it was suggested that, on the basis of observed differences between the two groups, initiatives be taken by post-secondary institutions to address the apparent lack of awareness and attention that students appear to pay to their potential risk. It was also suggested that, given the overall level of naivety in both groups, provincial and federal government agencies, as well as businesses (e.g., the Canadian Bankers Association), need to explore educational and legislative measures to better inform and protect consumers, regardless of their age, gender, and life experiences.

So while much has been said in the media about identity theft and identity fraud, there is a need for more detailed research to better

guide educational initiatives, assist law enforcement, and provide clearer direction for government and private sector efforts to combat the problem for different sectors of the population. Any effort to reduce identity theft will require a multi-pronged approach involving legislative changes, reporting structures, and public education.

Notes

We would like to acknowledge and thank the anonymous reviewers of our submission for their constructive feedback. We would like to acknowledge the support and assistance of our two research assistants, Beau Aktins and Jessica Woods. They were instrumental in the data collection and data entry, as well as identifying a few “glitches” in the survey. We would also like to acknowledge the voluntary assistance of Kristi Adams, who helped with aspects of the article, and Doug King, who was kind enough to offer feedback to the revised article.

1. In June 2006, the Montreal police dismantled a large debit card fraud ring that may have involved 18,000 victims in the Montreal area alone. According to the Interac Association, “Canadians use their debit card more per capita than anywhere else in the world” (Cherry and Legatos 2006: A8).
2. A recent RCMP publication (2006) notes that, unless required for a specific purpose the same day, you should never carry your SIN, birth certificate, and passport on you at the same time.
3. Most of the identity-theft cases related to credit cards or false application of credit cards (32%), while cell phones or false application for cell phones accounted for 12% of all identity-theft-related cases. The numbers reported by PhoneBusters, however, represent only calls received and not actual figures. That is, the numbers are dependant on people calling in, creating the potential for a sizable “dark figure” of unreported cases.
4. Consumer Sentinel has been collecting complaints since 2003 and every year the age group 18–29 had the highest proportion of complaints, followed by the 30–39 age group.
5. For example, the US “9/11 Commission Report” devotes only about 10 pages to addressing the deeply connected problems of terrorism and identity fraud (Sullivan 2004).

6. In 2000 a former Ontario immigration judge was charged with illegally "selling" Canadian visas to aid the illegal migration of Chinese families (Ronderos 2002).
7. The practice of phishing first came to the public's attention around 1996 and has since become a major technique for defrauding unwary victims. An example of recent phishing attempts involves scams to target customers of banks, eBay and PayPal and other online payment services. A customer will be sent an email on what appears to be authentic bank letterhead (but are in fact fake) requesting confirmation of personal information because of a possible breach of the clients account. Should the "victim" disclose personal information, it is then used to access the client's account or be used for other fraudulent purposes.
8. Drawing on a variety of sources, Smick (2006) notes that the number of undocumented immigrants into Canada is between 100,000 and 200,000 people. Since there are limited resources to enforce immigration laws and the hiring of undocumented workers, there is a very real risk that any number of such individuals are sharing their identity with legitimate residents who are not even aware of it.
9. Huopio (1998: 1) lists a host of techniques that are readily available and that he considers "cost-effective, reliable and highly accurate." They include using security measures that unequivocally identify a person through physical characteristics such as the iris, retina, face, fingerprints, or voice recognition. These physical characteristics are preferred as opposed to behavioural indicators, such as signature and typing rhythm.
10. In 2007, a number of Canada's major airport authorities were "backing efforts by an air industry coalition to pressure Transport Minister Lawrence Cannon to adopt a biometric screening program" that would facilitate people moving through airport security (Weeks 2007).
11. Government and general businesses were a distant second and third.
12. Perkins (2005) points out that "one in six consumers . . . say they have bought a privacy protection product to help avoid identity theft."
13. The CIPPIC White Paper addresses the need for legislation in Canada to protect individuals when their personal information has been compromised as a result of a breach within an organization's security. The paper calls for an amendment to the PIPEDA.

14. By contrast, in 2007, more than 30 American states had breach-notification laws.
15. SurveyMonkey was an online survey subscription survey in which we were able to provide the public with a website address to access the survey at any point throughout the duration of data collection.
16. Although some of the students could be considered citizens because of their age, we chose to differentiate the sample based on what the respondents were doing at the time of the survey and the fact that all students were registered as full-time students.
17. A copy of the survey is available upon request from the first author.
18. A similar search for the term "fraud" produced 697 articles for the month of January, 2007; 13,537 for 2006 and 17,583 for 2005!

References

- Allison, S.F.H., A.M. Schuck, and K.M. Lersch
2005 Exploring the crime of identity theft: Prevalence, clearance rates, and victim/offender characteristics. *Journal of Criminal Justice* 33(1): 19–29.
- Baum, K.
2006 Identity theft, 2004. Bureau of Justice Statistics Bulletin. Washington, DC: U.S. Department of Justice.
- Bohm, R.M.
1990 Death penalty opinions: A classroom experience and public commitment. *Sociological Inquiry* 60(3): 285–297.
- Brennan, B.
1999 March 22. Fraud squad: Calgary seniors tell their peers how to protect themselves against scams, cons. *Calgary Herald*, B6.
- Brown, B., and W.R. Benedict
2005 Classroom cops: What do the students think? A case study of student perceptions of school police and security officers conducted in an Hispanic community. *International Journal of Police Security Management* 7: 264–285.

Bureau of Justice Statistics

- 2007 Public attitudes towards crime and criminal justice-related topics. http://www.albany.edu/sourcebook/tost_2.html.

Cabinet Office

- 2002 Identity fraud: A study. London, UK: Cabinet Office Canadian Centre for Justice Statistics. See CCJS.

Canadian Internet Policy and Public Interest Clinic

- 2007 Approaches to security breach notification: A White Paper. http://www.cippic.ca/documents/bulletins/BreachNotification_9jan07-web.pdf.

CCJS

- 2000, 20(10) Criminal Victimization in Canada, 1999.

Cherry, P., and J. Legatos

- 2006 June 21 Montreal police dismantle large debit credit card fraud ring. Calgary Herald, A8.

Cherry, T.

- 2005, August 18 Identity theft can leave victims in ruin. Calgary Herald, B3.

Chua, J.

- 2003 Identity theft: Robbery in the new millennium. CBC News. <http://www.cbc.ca/consumers/indepth/identity/> (accessed November 7, 2006).

Consumer Measures Committee

- 2005 Working together to prevent identity theft. [http://cmcweb.ca/epic/site/cmc-cmc.nsf/vwapj/Discussion%20Paper_IDTheft.pdf/\\$FILE/Discussion%20Paper_IDTheft.pdf](http://cmcweb.ca/epic/site/cmc-cmc.nsf/vwapj/Discussion%20Paper_IDTheft.pdf/$FILE/Discussion%20Paper_IDTheft.pdf).

Consumer Measures Committee

- 2006 Watch your identity: Tips for reducing the risk of identity theft. <http://cmcweb.ca/epic/site/cmc-cmc.nsf/en/fe00040e.html>.

Criminal Intelligence Service Canada

- 2007 Identity theft. http://www.cisc.gc.ca/annual_reports/annual_report2005/identity_theft_2005_e.htm.

Dart, B.

- 2005 March 5 Terrorist access to database feared. Atlantic Journal-Constitution. <http://billnelson.senate.gov/news/details.cfm?id=244300&>.

DeGroote School of Business

2007 Defining and measuring identity theft in Canada. <http://www.business.mcmaster.ca/IDTDefinition/index.htm>.

Federal Trade Commission

2006 Consumer fraud and identity theft: Complaint data, 2005 January–December. Washington, DC: Federal Trade Commission, Sentinel and the Identity Theft Data Clearinghouse.

Gaudin, S.

2005 Taking on cyber crime's new mob ties. <http://www.esecurityplanet.com/trends/print.php/3487751>.

Giacopassi, D., M. Vandiver, and B.G. Stitt

1997 College student perceptions of crime and casino gambling: A preliminary investigation. *Journal of Gambling Studies* 13(4): <http://www.springerlink.com/content/v32252188q50gv96/>.

Gordon, G.R., and N.A. Willox, Jr.

2005 Using identity authentication and eligibility assessment to mitigate the risk of improper payments. *Journal of Economic Crime Management*. <http://www.utica.edu/academic/institutes/ecii/publications/articles/BA37B29D-0238-FBEB-F4D047243B1A0BA4.pdf>.

Gordon, G.R., N.A. Willox, Jr., D.J. Rebovich, T.M. Regan, and J.B. Gordon

2004 Identity fraud: A critical national and global threat. *Journal of Economic Crime Management*. <http://www.utica.edu/academic/institutes/ecii/publications/articles/BA2C8FE1-D0EC-26B6-50870F45EA5CC991.pdf>.

Henderson, P.

2005 Businesses get wakeup call on identity theft. *Business Edge* 1(25): 1–2.

Hensley, C., A.J. Miller, R. Tewksbury, and M. Koscheski

2003 Student attitudes towards inmate privileges. *American Journal of Criminal Justice* 27(2): 249–262.

Higgins, G.E., T. Hughes, M.L. Ricketts, and B.D. Fell

2005 Student perception and understanding of identity theft: "We're just dancing in the dark". *Law Enforcement Executive Forum* 9(5): 163–178.

Hoar, S.B.

2001 Identity theft: The crime of the new millennium. *USA Bulletin* 49(2): http://www.usdoj.gov/criminal/cybercrime/usamarch2001_3.htm.

Home Office Steering Committee

- 2006 Identity theft: Don't become a victim. <http://www.identity-theft.org.uk/>.

Huopio, S.

- 1998 Biometric identification. Helsinki University of Technology: Dept. of Computer Science. <http://www.tml.tkk.fi/opinnot/tik-110.501/1998/papers/12biometric/biometric.htm>.

Institute of Education Sciences

- 2005 Indicators of school crime and safety: 2005. <http://nces.ed.gov/programs/crimeindicators/crimeindicators2005/indicators.asp?pubpage>.

Lemert, E.

- 1953 An isolation and closure theory of naïve check forgery. *Journal of Criminal Law and Police Science* 44: 297–298.

Lombardi, R.

- 2006 March 22 Myths about identity theft debunked by experts. *IT World Canada*. <http://www.itworldcanada.com/a/News/e161e83b-f2b4-4aba-bff4-44d22b0ee696.html>.

Mackey, D.A., and Courtright K.E.

- 2000 Assessing punitiveness among college students: A comparison of criminal justice majors with other majors. *Justice Professional* 12(3): 423–441.

MasterCard

- 2006 PYID: Protect your I.D.; MasterCard survey shows Canadians need to guard their personal information. <http://www.newswire.ca/en/releases/archive/march2006/09/c0473.html>.

Mayer, E.

- 2005 ID theft victims face lots of work. http://www.contracostatimes.com/ml/d/cctimes/business/personal_finance/11071320.

McPhie, P.

- 1996 Fraud. In L. W. Kennedy and V. F. Sacco (eds.), *Crime Counts: A Criminal Event Analysis*. Scarborough: Nelson.

Mesko, G., P. Umek, and K. Musek

- 1996 Students' attitudes toward the police in Slovenia. <http://www.ncjrs.gov/policing/stu531.htm>.

Miller, A., R. Tewksbury, and C. Hensley

2004 College students' perceptions of crime, prison and prisoners. *Justice Professional* 17(3): 311–328.

Milne, G.R.

2003 How well do consumers protect themselves from identity theft? *Journal of Consumer Affairs* 37(2): 388–402.

Ministry of Government and Consumer Services

2008 Protecting your identity. http://www.gov.on.ca/MGS/en/ConsProt/STEL02_045993.html.

Moneris Solutions: Canada's Credit and Debit Card Processing Experts

2006 <http://www.bcroialbank.com/merchantservices>.

MyTruston

2007 Identity theft facts. http://www.mytruston.com/resources/identity_theft_facts.html.

O'Brien, T.

2004 October 24 Identity theft is epidemic: Can it be stopped? *New York Times*, s. 3, p. 1.

Perkins, B.

2005 March 31 Consider protecting your own identity. *Reality Times*. http://realitytimes.com/rtpages/20050901_protect_identity.htm.

Perkins, H.W., Meilman, P.W., Leichter, J.S., Cushin, J.R. and Presley, C.A.

1999 Misperceptions of the norms for the frequency of alcohol and drug use on college campuses. *Journal of American College Health* 47(6): 253–259.

Perkins, T.

2007 March 8 A crime that can touch us all. *Toronto Star*. <http://thestar.com.printarticle/188464>.

Peterson-Badali, M., and C.J. Koegl

1998 Young people's knowledge of the Young Offenders Act and the youth justice system. *Canadian Journal of Criminology* 40(2): 127–152.

Public Safety

2008 Identity theft: Questions and answers. http://www.safecanada.ca/identitytheft_e.asp.

RCMP

2006 Personal information and scams protection: A student practical guide. http://www.rcmp.ca/scams/student_guide_e.htm.

RCMP

2007 Identity theft. http://www.rcmp-grc.gc.ca/scams/identity_theft_e.htm.

Robinson, M.B.

1999 What you don't know can hurt you: Perceptions and misconceptions of harmful behaviors among criminology and criminal justice students. *Western Criminology Review* 2(1): <http://wcr.sonoma.edu/>.

Ronderos, J.G.

2000 May 31–June 1 Identity fraud and transnational crime. Paper presented at the Seventh Meeting of the CSCAP Working Group on Transnational Crime, Manila. http://www.ncjrs.gov/nathanson/id_fraud.html.

Saffran, D.

2005 October 6 Canadians and identity theft: Concern on the rise. <http://www.ccnmatthews.com/news/releasesfr/show.jsp?action=showrelease&actionfor>.

Shamlan, J.

2005 Main culprit in kids' ID theft? Family members. <http://www.msnbc.msn.com/id/7045490>.

Slitz, J.

2004 Fighting economic crime with a resolved identity platform. *Journal of Economic Crime Management* 2(2). <http://www.utica.edu/academic/institutes/ecii/publications/articles/BA3039FB-CFEB-450F-00BB282E916844D1.pdf>.

Smick, E.

2006, July 6 Canada's Immigration Policy. http://www.cfr.org/publication/11047/canadas_immigration_policy.html?breadcrumb=%.

State of the net 2006

2007 http://www.consumerreports.org/cro/electronics-computers/online-protection-9-06/state-of-the-net/0609_online_prot_state.htm.

Stewart, S.

2007, January 25 Winners security breach hits home. *Globe and Mail*, A1.

Sullivan, B.

2004, August 4 9/11 report light on ID theft issues. <http://www.msnbc.msn.com/id/5594385>.

Sullivan, M.

1997 Student perceptions of campus alcohol and drug use at the University of North Carolina at Chapel Hill. 152.19.4.9/wrkunits/3ctrpgm/alcohol/prevention/perception.html.

Towle, H.

2004 Identity theft: Myths, methods, and new law. *Rutgers Computer and Technology Law Journal* 30: 237–325.

Trembley, P.

1986 Designing crime: The short life expectancy and the workings of a recent wave of credit card bank frauds. *British Journal of Criminology* 26: 673–690.

United States Department of Justice

2005 Identity theft and identity fraud. <http://www.usdoj.gov/criminal/fraud/idtheft.html>.

Victim Assistance Online

2007 Fraud and identity theft. <http://www.vaonline.org/fraud.html>.

Walters, N.

2006, July Into the breach: Security breaches and identity theft. http://www.aarp.org/research/frauds-scams/fraud/dd142_security_breach.html.

Ward, S.

2005 Identity theft frauds becoming more serious. <http://sbinfocanada.about.com/b/a/151897.htm>.

Weeks, C.

2007, April 23 Scans could speed travel. *Calgary Herald*, A1.

Copyright of *Canadian Journal of Criminology & Criminal Justice* is the property of University of Toronto Press and its content may not be copied or emailed to multiple sites or posted to a listserv without the copyright holder's express written permission. However, users may print, download, or email articles for individual use.