

IDENTITY THEFT

Personal identity theft is the unauthorized collection and fraudulent use of someone else's personal information. It is the fastest growing white-collar crime in North America, and it is largely preventable. Consumers need to understand the problem – how identity can be stolen, how to recognize the signs of becoming a victim, and most importantly, what steps to take to protect oneself. The emotional and psychological costs to identity theft victims are significant, and, on average, victims will spend 600 hours and approximately US\$1400 clearing their names and cleaning up their credit histories.¹

In 2004, 13,000 Canadians reported \$20 million in losses to identity theft crimes.² In 2003, almost \$1.3 million was taken from Alberta victims. Nationally, 2003 and 2004 were comparable both in terms of victims and losses reported; however, losses to Canadians almost doubled from 2002 to 2003. PhoneBusters figures are only the “tip of the iceberg” as most occurrences of identity theft remain significantly underreported. The Canadian Council of Better Business Bureaus estimates that identity theft costs at least \$2.5 billion a year to the Canadian economy.³

According to the Federal Trade Commission in the United States, identity theft has been the top fraud complaint reported by consumers since 2000, with 246,570 people registering complaints in 2004⁴ and a total economic cost of US\$52.6 billion.⁵ However, some surveys suggest that the actual number of identity theft victims in the US could be as high as 10 million annually.⁶ In the UK, more than 100,000 people are affected by identity theft annually costing the British economy an estimated £1.3 billion per year.⁷

The 2005 Identity Theft Index Canada survey indicated that eighty percent of Canadians think identity theft is a serious problem; an increase of one third in just one year. One in

¹ Identity Theft Resource Center, *IDENTITY THEFT: THE AFTERMATH 2003 A Comprehensive Study to Understand the Impact of Identity Theft on Known Victims*, September 2003.

² PhoneBusters, *Identity Theft Statistics*, http://www.phonebusters.com/english/statistics_E03.html.

³ CBC News Special Report, *Identity Theft – Robbery in the New Millennium*. November 7, 2003.

⁴ Federal Trade Commission, *FTC Releases Top 10 Consumer Complaint Categories in 2004*, February 2, 2005.

⁵ Javelin Strategy & Research, *2005 Identity Fraud Survey Report*, January 2005.

⁶ Federal Trade Commission, *Federal Trade Commission – Identity Theft Survey Report*, September 2003.

⁷ Home Office Identity Fraud Steering Committee, <http://www.identity-theft.org.uk/>.

four Canadians reported that they personally, or someone that they know, have been a victim of identity theft. Unauthorized credit card purchases are the most frequent, but least costly form of identity fraud, accounting for seventy percent of reported cases. However, other forms of identity fraud, including takeover of existing credit card accounts (43%), the opening of new credit card accounts (36%) or new loans (22%), unauthorized bank account access (42%) and the use of the victims' personal information in other types of frauds (24%), are resulting in greater losses for consumers.⁸

The majority of identity theft fraud in Canada (34%) is being self-detected by individuals reviewing their own bank or credit card statements or credit reports. Thirty percent of victims report that their bank or credit card company first detected the fraud. Given the increases in both the incidences and costs of identity theft, it is not surprising that Canadians are expecting more from themselves (92%) in terms of protection, as well as from banks (87%), credit card companies (84%) and government (79%).⁹

The most common forms of identity theft worldwide include credit card fraud, phone or utilities fraud, and stealing funds from existing chequing, savings, or investment accounts.¹⁰ However, a rapidly emerging vehicle for committing identity theft is the Internet. Computers and the Internet have allowed identity thieves to obtain personal identifiers of multiple persons quicker; to access higher quality fake identification tools; and, through e-commerce, to render the credit transaction completely impersonal.¹¹ Tools such as digital certificates/digital signatures, biometrics and authentication do exist and could be employed to limit future Internet identity theft damage.

Albertans see privacy, identity theft and fraud as critical issues for government to address. In response to these issues, the Alberta government introduced a new, more secure driver's licence in 2003; developed the *Personal Information Protection Act* (PIPA) to protect the privacy of Albertans in the private sector in 2004; and with its partners, created a universal identity theft statement to provide victims with a single form for notifying banks, retailers and credit card issuers of stolen identity.

⁸ Identity Theft Index Canada, <http://www.tmcnet.com/usubmit/2005/Feb/1120734.htm>

⁹ Ibid.

¹⁰ Federal Trade Commission, *National and State Trends in Fraud and Identity Theft*, February 1, 2005.

¹¹ Thomas A. Hemphill, *Identity Theft: A Cost of Business?*, *Business and Society Review* 106:1, 2001, 51-63.

The federal government has responded to Canadians by amending the *Personal Information Protection and Electronic Documents Act* (PIPEDA). This Act requires organizations in the private sector to obtain the individual's knowledge and consent before using or disclosing personal information for a purpose not originally consented to. In addition, consumers cannot be denied a product or service if they refuse to provide their Social Insurance Number (SIN) in circumstances where it is not required by law.

In spite of these federal and provincial acts, Canadian law with respect to "personal information" and "identity" remains significantly weaker than in the United States and should be reviewed to provide greater protection for consumers. The Criminal Code does not yet view identity as "currency" in spite of the shift to identity based accounts for monetary exchange. Revising the Criminal Code sections that address theft and fraud to also apply to identity is a critical first step in enhancing our approach to the issue. AMA members support revisions to the Criminal Code to deal with identity theft. In this year's Member Opinion Survey, 95% expressed support for the introduction of a criminal code offence for people who have multiple identification documents in their possession.¹²

In May 2003, the Government of Canada identified the five most common methods of identity theft in Canada.¹³ They include:

- 1) *Theft of payment cards and documents*: identity thieves often steal purses or wallets, and steal newly issued cards or pre-approved credit card applications from residential mailboxes. Some, known as "dumpster divers," will even rummage through trash at residences and businesses to pick out bank and credit card information. The good intentions of blue box style recycling initiatives offer enormous opportunities to identity thieves.
- 2) *Shoulder surfing*: Some identity thieves look over your shoulder, observe from a nearby location, or take a picture with a camera phone as you enter your PIN at an ATM machine. By installing a fake ATM device that reads your card's encoded data, or by distracting you while your card is taken or switched with

¹² AMA Member Opinion Survey 2005.

¹³ Public Safety and Emergency Preparedness Canada. *Public Advisory: Special Report for Consumers on Identity Theft*, May 21, 2003.

another, an identity thief can then use your PIN to drain your bank account without your knowledge.

- 3) *Card skimming*: Identity thieves also “skim” or “swipe” customer credit cards at restaurants or cash stations, using an electronic device known as a skimmer. Identity thieves then transfer or transmit those data to another location where it is re-encoded onto fraudulently made credit cards.
- 4) *“Phishing” and “Spoofing”*: The creation of e-mails and websites that appear to belong to legitimate businesses, such as financial institutions or online auction sites. Consumers who receive e-mails claiming to be from a legitimate business are often directed to a website at which the consumers are directed to enter large amounts of personal data. The sole purpose of these websites is to obtain the consumers’ personal data to engage in various fraud schemes. In addition, “Trojan” virus programs that collect personal information without the user’s knowledge, as well as the use of keystroke recorders that can be installed on individual computers are becoming increasingly widespread.
- 5) *Theft from databases*: There has been a significant increase in efforts by identity thieves to access large databases of personal information that private companies and government agencies maintain. Criminals have broken into offices to steal computer hard drives, bribed or compromised employees into obtaining personal data for them, and hacked into databases.

Consumers can prevent the first four methods of identity theft from occurring if they have been informed about personal information practices such as: protecting personal information, securing mail, and securing accounts. It should be the role of financial institutions, credit bureaus, governments and consumer groups, such as the AMA, to improve both their internal policies and their consumer education efforts. In response to the fifth method of identity theft, the Government of Canada and Government of Alberta have established the 10 Principles of Privacy that all companies are required to adhere to. These 10 principles are listed in Appendix I.

It is important, however, that actions taken by government to stem the tide of identity theft do not unduly infringe upon individual privacy and civil liberties. It has been suggested that national identity cards with biometric identifiers, and integrated government databases could potentially reduce the incidence of identity theft. However,

these initiatives raise serious privacy issues, and should be subjected to thorough public consultation and debate.

A recent study revealed that 65% of Canadians would accept the use of biometrics such as fingerprinting or iris scanning as a way to verify identity. Reasons cited for using biometrics included increased security of information (89%), convenience, in that biometrics could eliminate the need to remember passwords (54%), and increased transaction speed (39%).¹⁴ As the use of biometrics becomes more widespread and the technology around it improves, Canadians will likely become more accepting of the use of the technology itself.

Investigating and prosecuting identity theft is difficult and costly. Law enforcement officials cite a number of challenges, including lack of an offence for simple possession of false or multiple identification documents, the expense of identity theft investigations, the inter-jurisdictional nature of many identity theft cases, and the need for inter-agency information sharing and cooperation.¹⁵ Compounding these challenges is the slow pace of federal initiatives to deal with the identity theft issue and revise how government documents are produced, used, accessed, and secured. Alberta, for its part, has made some significant change in terms of securing selected government issued documents, is examining best practices to improve the security of all documents used for identification and verification purposes, and is expected to establish a cross ministry initiative to examine the issue in detail.

AMA recognizes the importance of identity theft to both its members and the organization itself. AMA member opinion was gauged on the issue in 2005. Sixty-nine percent of members surveyed indicated that they feel some degree of vulnerability to becoming a victim of identity theft. Methods that members are taking to protect themselves from becoming victims include:

- Shredding personal documents when recycling or discarding (78%);
- Not responding to unsolicited emails (97%);
- Not dealing with unfamiliar financial organizations while on the Internet (98%);

¹⁴ Reid, P. and Brazeau, M., *EDS Canada Privacy and Identity Management Survey*, February 2005.

¹⁵ Lawson, P. and Lawford, J., *Identity Theft: The Need for Better Consumer Protection*, Public Interest Advocacy Centre, November 2003.

- Paying attention to people around them when using credit cards and bank cards (83%); and
- Not providing credit card or personal information over the phone to unsolicited sources (98%).

Only 24% of members register their credit cards with AMA or some other credit card registry. Almost all members surveyed (96%) believe that AMA has an important role to play in providing information or education about protecting their personal information.¹⁶

The AMA is directly affected by identity theft through the services that it provides to its members. As such, and in compliance with all governing privacy legislation, the AMA has developed a Privacy Policy that outlines its commitment to protecting personal information and the procedures in place to ensure that this information is protected. Other business practices that AMA has introduced include: a privacy complaint resolution process for members concerned about the use of their personal information, secure document shredding procedures for confidential documents and the truncation of credit card numbers on receipts. AMA is a recognized leader in this regard; however the organization is not immune to the risks of identity theft.

Theft of payment cards and documents is the most common form of identity theft in Canada. As an indication of the severity of the issues surrounding mail theft, the Government of Alberta, in consultation with its partners, is currently reviewing the delivery method (regular mail) of the new drivers' license. An effective delivery model for all important documents and cards should be timely, flexible, convenient, secure and trackable – and should not be the weak point in an otherwise secure process. It is likely that AMA Registry Services will be affected by changes associated with the new Alberta drivers' license.

The financial services provided by the AMA are also potentially at risk. For example, the AMA MasterCard issuers need to ensure that credit is not granted to identity thieves and that the AMA MasterCard does not end up in the hands of thieves when it is first delivered to the cardholder. The card does have around-the-clock fraud protection program designed to protect consumers.

¹⁶ AMA Member Opinion Survey 2005.

There have recently been several high profile incidences of company database theft. It is the AMA's responsibility to maintain the security of all company databases, including the registries database, and the integrity of the employees who have access to it. Any information leaks from these databases would be detrimental to AMA members and the AMA's reputation.

To ensure government action on identity theft and privacy adequately addresses the complexity of both the problem and consumer needs, the following policy was approved at AMA's 2005 Annual General Meeting.

THE GOVERNMENT OF ALBERTA IS ENCOURAGED TO DEVELOP A PROVINCIAL STRATEGY TO ADDRESS THE GROWING AND COMPLEX ISSUE OF IDENTITY THEFT THAT INCLUDES PUBLIC AWARENESS AND EDUCATION PROGRAMS TO INFORM INDIVIDUALS ABOUT IDENTITY THEFT. SUCH PROGRAMS SHOULD INCLUDE HOW TO RECOGNIZE IDENTITY THEFT, HOW TO MINIMIZE THE RISKS AND WHAT TO DO IF VICTIMIZED.

The following statements were also approved for referral to CAA:

THE FEDERAL GOVERNMENT IS URGED TO CONDUCT A THOROUGH REVIEW OF HOW THE CRIMINAL CODE AND THE PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS ACT (PIPEDA) DEAL WITH "PERSONAL INFORMATION" AND "IDENTITY". SECTIONS OF THE CRIMINAL CODE REFERRING TO THEFT AND FRAUD SHOULD BE REVISED TO ALSO APPLY TO IDENTITY.

GOVERNMENTS SHOULD AMEND EXISTING LEGISLATION TO REDUCE THE RISKS OF IDENTITY THEFT AND PROVIDE CONSUMERS WITH MORE EFFECTIVE PROTECTION AND REMEDIES.

APPENDIX I: The 10 Principles of Privacy

- 1) *Accountability*: Companies are responsible for personal information under their control.
- 2) *Identifying Purposes*: Companies must identify why information is being collected before it is actually collected.
- 3) *Consent*: Individuals must consent to the collection, use and disclosure of their personal information.
- 4) *Limiting Collection*: Personal information collected is limited to that which is necessary.
- 5) *Limiting Use, Disclosure and Retention*: Companies can not use or disclose personal information for purposes other than those for which the information was collected, and may retain information only for as long as necessary to fulfill the purposes for collecting such information.
- 6) *Accuracy*: Companies will maintain personal information in an accurate, complete, and up-to-date form as is necessary to fulfill the purposes for which it is to be used.
- 7) *Safeguards*: Personal information will be protected with security safeguards appropriate to the sensitivity of the information.
- 8) *Openness*: Companies will make readily available their policies and practices relating to the management of personal information.
- 9) *Customer Access*: Upon request, companies will inform individuals of the existence, use and disclosure of their personal information and will make this information available, subject to legal restrictions.
- 10) *Challenging Compliance*: Questions and inquiries concerning compliance are to be directed to the company's Chief Privacy Officer.