



terrANOVA
Identity Fraud

Constant references to identity theft are made by the media. The topic is even splashed across the front page of many publications. Many articles, blogs and even television news programs are dedicated to discussing identity theft. There are many information security firms that offer products to protect you against this phenomenon. Should you purchase them? Do you need to be concerned? What does identity fraud really involve?

First, identity theft is not the same as identify fraud. Identity theft occurs when someone assumes the identity of a dead person—who is in no position to contest the issue. Identity fraud means obtaining personal information that can be used to assume someone else’s identity. Identity fraud has become a common crime in Canada. Taking over the identity of a person or business is also an effective path to committing other crimes.



How does identity fraud work? The fraudster obtains important information on the victim, such as name, address, date of birth, social insurance number, mother’s maiden name, etc. The fraudster then “becomes” that person, gaining no-holds-barred access for example to the victim’s bank accounts. From that point on, the fraudster can open new accounts, transfer balances, apply for loans and credit cards or obtain other services, such as the purchase of a vehicle. In 2008 alone, 1.7 million Canadians were victims of identity fraud.

To achieve their goals, fraudsters employ different methods, including theft, wiretapping, phishing and dumpster diving. What is interesting is that the use of the Internet does not directly increase the risk of falling victim to identity fraud.

A study published in 2009 by the Canada Research Chair in Security, Identity and Technology helps demystify some common notions that the media have popularized about this type of crime.

Interesting Fact

Statistic on personal information theft

Many studies have actually revealed that a large share of personal information thefts are committed by employees who misappropriate and then illicitly exploit information they obtain from clients, patients and benefit recipients in the course of their work.



organized crime is deeply mixed up in such activities. “Internet use poses a threat to our identity.” More than 50% of all identity fraud cases involve little technological skill (pickpocketing and purse snatching, for example).

Web-based identity fraud generally concerns online purchases or credit line applications. Identity fraud can take many forms and includes a set of relatively sophisticated techniques, strategies and tools. The scientific literature defines three key steps in the identity fraud process:

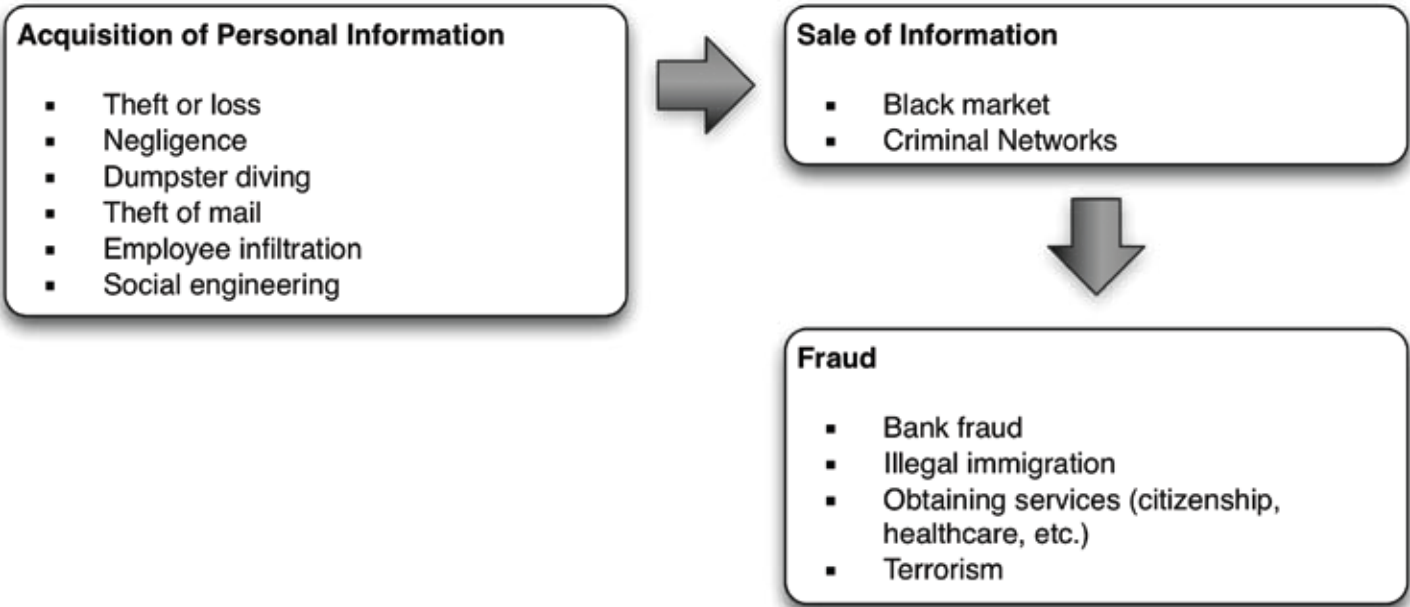
- * Acquisition of personal information,
- * Sale of that information,
- * Perpetrating fraud under an assumed name.

“Men are chiefly responsible for information theft.” The study reveals that women represent almost 40% of all identity thieves. Men and women are almost equally responsible for this type of crime.

“Young people are more likely to commit fraud using someone else’s identity.” The study also shows that the average age of offenders is slightly higher (33) than it is for other forms of crime. “Such acts are perpetrated primarily by foreign criminal organizations and organized groups.” In a majority of studied cases, fraud criminals act on their own, which would contradict the theory that

The following figure illustrates how this works:

Three Key Steps in Identity Fraud



The Internet, various forms of communication and associated technologies only typically come into play once the information is being sold and the fraud perpetrated.

The ingredients of the crime as described above illustrate that identity fraud is not an exclusively technological phenomenon. Somewhat less than 20% of all cases studied involve a theft of personal information over the Internet. This low percentage is probably due to the fact that those involved in such activities often operate on their own and when the opportunity arises. Their behaviour thus tends to be spontaneous and their means of acquiring information quite rudimentary. However, after they have acquired personal information, criminals enjoy using the Internet and similar forms of communication when actually committing their frauds.

Identity fraud is essentially an economic crime. Offenders are seeking to gain material wealth in a very large percentage of frauds. Identity fraud also plays an important role in illegal immigration. We will not consider this very complex social issue here in detail. Rather, we shall focus on how such fraud pertains to economic crimes.

Internet and new technologies are not at the root of most cases of identity fraud. However, a growing number of identity-related documents (social insurance numbers, driver's licences, credit cards, etc.), combined with an increasing online presence by a public largely ignorant about identity fraud, could cause a rise in the amount of identity theft that occurs over the Internet and with related technologies. If so, this would be due to inappropriate use by a poorly informed public, rather than to the Internet or to such technologies themselves.

We have little in the way of demographic statistics about identity fraud victims. Yet literature on the topic debunks the common myth that elderly individuals make up a disproportionately high number of victims. One underlying assumption seems to be that the less technosavvy are more vulnerable to con artists. More recent studies show, however, that the majority of identity fraud victims fall into the 18-34 year old bracket. In many cases, the perpetrator is also acquainted with the victim.

How then can we protect ourselves from identity fraud? The answer lies in education. If we are adequately informed of risks inherent in certain situations, we are more likely to address the issue. We are responsible for acquiring a better understanding of the ingredients that make up our identity and of protecting our personal information on a regular basis.

Do not give out personal information over the telephone unless you can identify the other party. Be wary of disclosing information unnecessarily. A landlord does not need your social insurance number to write a lease. Your SIN is only intended for government agencies. Do not reveal personal information to open a video club account or any type of account that is not a financial institution. Always shred documents containing personal information (credit card statements, etc.) before discarding them. When travelling, protect yourself against theft by only carrying the documents you really need. Act prudently when using the Internet and related forms of communication. Limit the amount of personal information you post on social networking sites such as Facebook.

Do not fall victim to this type of crime. Educating yourself on the inherent risks and following the simple rules stated above will go a long way in protecting your personal information.

References :

Benoît Dupont & Guillaume Louis, Les voleurs d'identité. Profil d'une délinquance ordinaire, Université de Montréal 2009.

Sproule, Susan et Norm Archer (2008). Defining identity theft. Eight World Congress on the Management of eBusiness, 11-13 juillet: Toronto.

Sproule, Susan et Norm Archer (2008). Measuring identity theft in Canada: 2008 consumer survey, MeRC working paper no. 23. McMaster University: Hamilton.

Allison, Stuart; Schuck, Amie et Kim Michelle Lersch (2005). Exploring the crime of identity theft: Prevalence, clearance rates, and victim/offender charac-

teristics. Journal of Criminal Justice, vol. 33, no. 1.

Identity Theft and Strategies for Crime Prevention, National Crime Prevention Council 2007-2008, United States Department of Justice and Bureau of Justice Assistance, PowerPoint document, www.ncpc.org



For Formation Terra Nova Inc.
Marc-André Fortier
Adviser, Strategic Communications
www.formationterranova.com

