

Identity Theft on the Rise – Scariest than Click Fraud

By Jim Hedger, StepForth News Editor, [StepForth Placement Inc.](#)

Many search industry observers see click fraud as the number one threat to the growth of the Internet economy. An even greater threat has emerged one that not only places the entire infrastructure of the Internet at risk, it also threatens non-Net users.

Identity theft has always been an issue in our economy, at least as long as there have been schemers and confidence scams. Before the advent of the commercial Internet, it would take a great deal of knowledge and skill to assume another's identity. It still does however; a decade into the age of the commercial Internet, accessing and making use of personal information has never been easier for cyber-criminals. Nearly everyone who uses the Internet has experienced an attempt by somebody somewhere to obtain personal identifying information. From phishing expeditions like the phony eBay and PayPal account update emails everyone receives to more complex methods such as the subtle installation of spyware, viruses and worms, criminals have found a nearly open range where they can exploit the carelessness or weakness of others with virtually no one to stop them.

In 2003, the US Federal Trade Commission noted that 1 out of every 25 adults in the United States was a victim of identity theft. That figure is two years old. Since then, we have seen stories about electronic break-ins and the theft of hundreds of thousands of pieces of personal information leak out from data storage and mining firms such as ChoicePoint and Lexis-Nexus. In comparison, the FTC estimated the number of Americans who were victims of credit-card fraud at about 1 out of every 20 in 2001.

ID theft is, according to FTC figures, the most popular and fastest growing form of consumer fraud. Over 2004, the FTC reported ID thieves took over \$100 million from financial institutions, or an average of \$6,767 per incident. For individual consumers, the numbers are even more staggering. As reported by Janet Wu of by Boston television station WCVB-TV, money stolen through identity theft amounted to over \$50 billion in the United States last year. In other words, nearly \$200 per US citizen was somehow stolen due to identity theft.

That was last year. This year the numbers are expected to rise dramatically. On June 20, CNN reported that a breach of security at a third-party processing firm exposed nearly 40 million credit card accounts to potential fraud. 22 million Visa card holders and a further 14 million MasterCard were accessed over time when hackers busted into Tucson based CardSystems Solutions and installed a script that searched out specific types of card transaction data. The intrusion was discovered and stopped on June 20 but not before the hackers managed to export information on over 130,000 unique card holders. Information gained included names, credit card numbers and personal security codes.

This is not only a concern for individual consumers and financial institutions. The massive increase in identity theft also presents significant national security issues. The criminals who steal and use other's identities tend to be highly organized and work in teams. For them, this is a business, not an avocation. When criminals can compile enough identifying information about individual citizens to ring up thousands of dollars against their credit or bank cards, what stops them from selling that information to terrorists,

foreign intelligence services or other organized criminals? Virtually nothing, as a recent report from Great Britain demonstrates.

Americans are not the only people in the world who are affected. On June 23, an undercover reporter from UK newspaper [The Sun](#), Oliver Harvey, wrote about how he purchased information on over one thousand British citizens, from a company in India. For less than five dollars per person, Harvey was able to obtain bank and credit card digits and pass-codes, addresses, driver's license info, and even passport registration numbers. Harvey's contact in India, a Kkaran Bahree claimed to be able to access and pass details from over 2000 accounts per month through a network of call center workers in Delhi.

It is astonishingly easy to steal personal information. What is even more astonishing is the apparent cavalier attitude shown until now by the major data storage and credit corporations who have all moved to close the barn door long after the horses have escaped. Recent laws passed in California and Illinois now put the onus on data storage firms to immediately inform consumers when a breach of personal data occurs. Before such laws, denial was often the first line of defense for many large data storage corporations.

Unfortunately, there is simply no way to secure electronic data from prying eyes. As any junior hacker will tell you, breaches in security are found as quickly as that security is established. The onus therefore remains on the consumer to take action to protect themselves and their personal information. A few years ago, consumers were told to shred all mail from financial institutions before disposing of it or recycling it. Shredding worked for paper documents but is somewhat more difficult for electronic ones. Today there are small steps consumers can take to protect themselves and knowledge is by far the best defense for individuals.

The first and most important thing for consumers to learn is their legal rights. For instance, many Americans don't realize that section 609(e) of the [Fair Credit Reporting Act](#) gives them the right to examine the signature on a contract to prove it is not their own. As long as you can provide legal proof of identity and a police report or affidavit, creditors have an obligation to provide copies of transaction records for your inspection.

A second thing consumers should do is monitor their credit reports. Credit reporting firms such as Equifax, TransUnion and Experian allow consumers to view their personal credit reports for accuracy and report inconsistencies. For US residents, the federal Fair Credit Reporting Act requires each of the major nationwide consumer reporting companies to provide consumers with a free copy of their credit reports, at their request, once every 12 months. This is as important as reviewing your monthly bank statement as criminals often wait months or even years to make use of personal identifying information.

Thirdly, it is important to compile as much documentation as possible to prove your case. Collection letters, previous credit reports, a legally notarized affidavit, and whatever other evidence you can gather will help when you make complaints to authorities. Since electronic identity theft is a relatively new twist on an old game, you might have to provide local police or other authorities with information about ID theft. You might need to remind them that a police report is necessary for the credit reporting agencies to take action. In some jurisdictions, state or provincial law does not yet cover identity theft. If that is the case, ask to file a miscellaneous incident report. If local authorities are unable or unwilling to help, you might need to take your case to state or provincial police forces or even federal policing agencies such as the RCMP or FBI.

Consumers should understand that creditors are becoming more knowledgeable about identity theft. While they might resist an easy settlement, it is in their best interest to communicate with and cooperate with the consumer. It is up to the consumer to provide as much information and proof of their innocence as possible. It is also up to the consumer to take measures to actively protect their personal data. Banks recommend changing your personal ID number (PIN) every three months. They also recommend that consumers become a bit more creative when choosing their PINs. When doing so, avoid using information that is easy to figure out, such as phone numbers, birthdates, or a series of consecutive numbers.

Most importantly, never stop learning about identity theft, how it can affect you and what you can do to protect yourself. If you don't already know the managers of your bank branch, this might be a good time to meet them, if only to put a face to your name in their minds. When your credit history is under attack, you have only your personal credibility to fall back on. Even in an increasingly electronically driven society, personal credibility relies on the strength of your relationships. This might be a good time to start building them or shoring them up.

Identity theft is a problem that is not going to go away soon. Even with the development of "smart-id" cards such as biometric identity cards, the most vulnerable financial transactions take place electronically where even the most stringent biometric information is absolutely useless. Consumers need to be aware that personal information is being collected by lots of entities; a lot more personally identifying information is being collected than we are aware of. As too many stories remind us, security is not always foolproof. It is up to you to protect yourself.

Here are some useful links designed to help victims of identity theft. They might help you avoid becoming one as well.

United States:

[Federal Trade Commission – Identity Theft](#)
[Privacy Rights Clearing House](#)
[US Department of Justice](#)

Canada:

[Office of the Privacy Commissioner](#)
[Canadian Credit Report](#)
[Canadian Privacy Law Blog](#)