ARTICLE
27 September 2003

Online Identity Fraud

PROFESSOR MARK GRIFFITHS*

In February 2000, a Boston medical-equipment supplier telephoned San Diego family doctor Ignacio Ramirez demanding payment of $85,000. It took him days to convince the company that he had never bought anything from them (Marlin, 2000). It then took weeks to learn that a woman had stolen his identity off the Internet. She took information from the Medical Board of California, his medical licence identification and Social Security numbers and used them to buy medical supplies on his credit. In total, $185,000 had been fraudulently spent.

Identity theft is one of the fastest growing white-collar crimes in the country and the likelihood of becoming a victim via an online attack is growing as criminals are becoming more persistent and difficult to stop. As many other types of crime are declining, identity theft is booming (Jopling, 2003). By stealing enough information to impersonate consumers, criminals are defrauding businesses of millions of pounds a year. One reason criminals steal identities is to mask their participation in a crime. The more convincingly a criminal can establish that they are someone else, the more likely it is the authorities will not come after that criminal.

Jopling (2003) says there are a number of reasons for the increase. Firstly, masses of consumer and business information are being put online every day to meet the requirements of businesses competing in very competitive environments. Secondly, despite the costs of fighting identity theft, the web is still cost-effective to businesses and consumers with advantages far outweighing disadvantages. The real issue is that most organizations cannot devote resources to keeping up with the criminals, let alone get ahead of them by designing systems that are so sophisticated that prevent criminals getting in.

Hammeed (2003) defines identity theft as the stealing of someone's personal data and using it to assume his/her identity. This act is often a precursor to credit card fraud (ie, setting up a new credit card account in someone's name based on stolen personal information). The real worry here is that the Internet technology provides tools to help criminals in new ways. Online identity thieves can steal personal information such as credit card numbers, social security numbers and other information. Through financial liability with credit cards may be limited (eg, $50 to $500) it can take years to sort out the mess that online identity thieves leave behind.

Identity theft remains the primary concern among consumers contacting the US Federal Trade Commission. According to two studies published in July 2003 (reports by Gartner Research and Harris Interactive), approximately seven million Americans became victims of identity theft in the prior 12 months (Identity Theft Center, 2003). The incidence of victimization increased 11 -20 *per cent* between 2001-2002 and 80 *per cent* between 2002-2003 (Harris Interactive, 2003; cited by Identity Theft Center, 2003). Furthermore, 49 *per cent* also stated that they did not feel they knew how to adequately protect themselves from this crime. The Harris Interactive study also claimed that 16 *per cent* of the respondents reported that the perpetrator was a co-worker, friend or family member. The US Federal Trade Commission reported in January 2003 that identity theft topped the list of fraud complaints reported by consumers in 2002, with some 163,400 of such complaints received by the agency (Wrolstad, 2003).

It estimated that the average identity theft crime costs the business community about £10,000 per victim (not including victim time lost from work, legal assistance, and judicial and law enforcement time in investigating and trying cases). On average, victims spend over 175 hours and other out-of-pocket expenses to clear their names (US Federal Trade Commission, 2002; quoted by Identity Theft Center 2003). Preliminary studies appear to indicate that the majority of identity theft criminals are repeat offenders with a wide range of other convictions (eg, substance abuse, violent crime). The bad news is that the average arrest rate is under five *per cent* of all reported cases by victims (Identity Theft Center, 2003).

It is very easy to steal someone's identity. The key is in the numbers that have come to identify all of us. A person's online identity consists of numbers and other information that describes them. If someone can use a social security number and link it to financial information (eg, bank account number, credit card number), they can begin to build an identity of someone online who has a lot of that person's characteristics. Reaves (2002) has outlined three basic ways to authenticate identity. Put very simply these are (i) something you know (eg, password, PIN number), (ii) something you have (eg, cashpoint card, job ID card) and (iii) something you are (handwriting, fingerprint). Anyone who understands identity theft knows these things. If they can get hold of this information, they can fake someone's identity.

It may also be the case that some online crimes are merging. For instance, the *Washington Post* (2003) reported the case of a Los Angeles 17-year-old who used fake web pages *(America Online* member pages) to lure consumers to provide credit card numbers and other personal data. He ran up $8,000 worth of debts by using the credit data he had obtained. The case against the teenager (who was not identified) was the first brought by the US Federal Trade Commission that targeted "phishing" - a scam that merges e-mail spam with identity theft. "Phishing" is the term is used by hackers to describe the act of fishing for information. "Phishers" send fraudulent e-mails to unsuspecting customers of service providers or retailers with whom consumers regularly do business. The e-mails

* Psychology Division, Nottingham Trent University.

are doctored to look like they came from the provider and claim that they need the consumer to verify his or her account information. Consumers are then asked to click on a link that directs them to a "'phisher" page, which is designed to mimic the service provider's site. The page asks the user to resubmit his or her personal information for the account, sometimes including passwords and Social Securiry numbers. The information is then used it to make purchases, set up bank accounts and steal a person's identity.

Many firms have been targeted including *Earthlink, eBay,* its payment subsidiary *PayPal,* and electronics retailer *Best Buy.* As a consequence, in September 2003, a number of high profile companies set up the *Coalition on Online Identity Theft* including *Amazon.com, eBay, Visa* and *Microsoft.* Identity theft has hurt online consumer confidence, and also has had a detrimental effect on the credibility of major online retailers like *Amazon.com and eBay* primarily through the increased use of "spoof" sites. These companies admit there is no simple solution but acknowledge it is important to bring big retailers and IT vendors together to develop better technological solutions to the problem. They also want to make sure law enforcement agencies increase the penalties for those found guilty of identity theft.

Identity theft has become one of the biggest problems in the current online era. This criminal epidemic not only poses a risk of financial loss in the most obvious sense but also inflicts a repurational damage due to ineffective Internet security (Hameed, 2003). With rapid expansion of real-time Internet transactions, the online fraudulent activities are fast becoming threat to the existence of web merchants, financial services companies, and the Internet customers. Web businesses are at serious risk with regard to their online privacy and security. Analysts fear cyber security attacks will hamper the growth of online commerce since the loss from fraud might outweigh the benefits brought by the Internet (ie, convenience, transparency, and immediacy). If this trend is not reversed, the industry might suffer huge financial losses.

Prevention and the Way Ahead

Experts believe the next generation of secure credit card payment systems to be much effective (Hameed, 2003). Solutions and services such as *Verified by Visa* and *Secure Code* (the *MasterCard* alternative), are considered easier for consumers since they require using only a password. Moreover, the credit card companies are offering coverage of the cost of online fraud ro encourage retailers to adopt more secure payment systems. According to Hameed (2003) there needs to be a coherent, industry-wide effort to fight insidious new technologies. These unscrupulous innovations are constantly waiting for the right trigger to perform their tasks. Based on such a situation, following preventative measures are important for the Internet users who trade commercially online (adapted and expanded from Edwards [2003]):

- Pay attention to the nature of product or service that asks for information about identity.
- Make sure the company is reputable and conforms to industry standards for ensuring content privacy and security (tools and guidelines).
- Keep focus on what kind of information is being shared.
- Never give mother's maiden name and social security number to anyone.
- Be wary of unsolicited e-mail that asks for personal financial or identity information (eg, Social Security numbers and/or passwords). Don't click on the links provided in such e-mail.
- When updating account information use a familiar process, such as visiting the known web address of a company's account maintenance page. Unfamiliar addresses for this probably are fake.
- Make sure an Internet connection is "secure" (with an icon of a lock visible on the web browser) before submitting personal information.
- Monitor credit card and bank statements for unauthorized charges.
- If an e-mail or web site is in doubt, make sure the request is authentic by contacting the company directly by phone or through a web site or e-mail address known to be authentic.
- Using credit cards is generally safer than allowing access into other accounts. The credit card system has safeguards built in to protect users from fraud. If someone steals a credit card number the credit card holder is only liable for a small amount of money. With a debit card, a person can have their account cleaned out completely.
- Credit card numbers and social security numbers should never be used to make charitable contributions.
- Never give out any identity information over the phone, particularly to anyone who has called you.
- Try to avoid writing bank account numbers on anything.
- Never give out social security number, online or otherwise. No company from which things can be bought needs a social security number.
- Additionally, never give out information such as birthday, marital status, education level or other personal information. This additional information makes it extremely easy for criminals to make themselves appear legitimate when they pose as you. Criminals prey on people's ignorance and can usually be defeated by making it too hard for them to get information.
- Use a good anti-virus program. Criminals can get credit card numbers, passwords and other sensitive information through "Trojan horse" viruses that log keystrokes and transmit information to criminals.
- Victims should immediately contact the police and get legal help. Do not wait because of embarrassment or stupidity over what happened. Waiting only lets the trail grow cold and limits how much law enforcement can help.

References

Edwards, J. (2003) "How to Prevent Online Identity Theft". Article located at: http://www.directsalesmarketingonline.coni/articles/je/identitytheft.html

Hammeed, I. (2003) "How Identity Theft Leads to Online Fraud." June 6. Article located at: http://internet.about.com/cs/whatneedtoknow/a/aa_id060303.htm

Identity Theft Center (2003) Facts & statistics (on identity theft). Located at: http://www.idtheftcenter.org

Jopling, P. (2003) "Tackling the Growing Problem of Online Identity Theft". Article located at: http://www.infosecnews.com/opinion/2003/06/18 01.htm

Marlin, A. (2000) Online identity fraud a growing problem. CNN.com August 16. Article located at: http://www.cnn.com/2000/TECH/computing/08/16/id.theft.offline.idg/

Reaves, J. (2002) "Identity Theft: Could it Happen to You?" *Time.* January 23. Article located at: http://www.time.com/time/nation/article/0,8599,196857,00.html

Washington Post (2003) "Online Identity - Theft Tactic Targeted". July 21. Article located at: http://www. washingtonpost.com/wp-dyn/articles/A25491 -2003 Jul21 .html

Wrolstad, J. (2003) "Coalition Targets Online Identity Theft." News Factor Network, September 3. Article located at: http://www.newsfactor.eom/perl/story/22209.litml#story-start