Identity theft – debilitating, and on the increase

Report by Eugene Oscapella

ID THEFT HAS BEEN A PROBLEM in the US for some time, and is now moving onto the world stage. Many businesses may still be unprepared, in terms of both organisation and technology, to deal with the problem.

Identity theft encompasses a broad range of fraudulent activities carried out under an assumed identity. The US General Accounting Office (GAO), the investigative arm of US Congress, describes identity theft (or identity fraud) as "stealing" another person's personal identifying information - such as government issued identifying numbers, date of birth, and mother's maiden name – and then using the information to fraudulently establish credit, incur debt, or take over existing financial accounts.

A May 8th article in *The Times* (UK) spoke of identity theft as the fastest growing fraud in Britain. US Attorney General John Ashcroft made a similar comment only days earlier about identity theft in the United States. However, a March 2002 report by the GAO cautioned that it is difficult to fully or accurately quantify the prevalence of identity theft, since no single hotline or database captures the universe of identity theft victims. Some individuals do not even know that they have been victimised until months after the fact, and some known victims may choose not to report to the police, credit bureaus, or established hotlines.

Still, the GAO concluded that although not specifically or comprehensively quantifiable, the prevalence and cost of identity theft seem to be increasing. Privacy author, Simson Garfinkel, in *Database Nation* (reviewed on p.31), suggests that there were between 500,000 and 750,000 cases of identity theft in the United States in 2000.

CRIME OF STEALTH

Recent testimony before the US Senate Committee on the Judiciary exposed the nature and depth of the problem in the United States. Given the ease with which personal financial information crosses borders, and the frequency of international financial transactions, this is much more than a domestic fraud problem.

Credit card fraud is a typical form of identity theft. A person might use the credit card of another person, or apply for and receive a new credit card in the victim's name. If a new card is issued, the victim will have no way of knowing that the card has been issued, since the victim will not receive a monthly statement for that card. Other forms of identity theft include the unauthorised use of telecommunications or utility services, writing fraudulent cheques, opening new bank accounts in the victim's name, making unauthorised electronic withdrawals, and securing personal, student, business, real estate or automobile loans. In some cases, identity thieves use the victim's identity for employment purposes or to obtain government benefits or medical services. Identity theft has even darker implications, since terrorists may seek to assume the identity of other individuals to facilitate their actions.

"Hijacking someone's identity using personal information such as social security or credit card numbers is the crime that vividly illustrates why consumers care about their privacy."

Timothy Muris, Chairman, FTC, speaking at the Twelfth Conference on Computers Freedom and Privacy, San Francisco, April 17th 2002

Identity theft operates by stealth, unlike many crimes where the commission of the crime is quickly apparent – car thefts or burglaries, for example. Victims of identity theft may go months or years without knowing that their identity has been stolen. About 5 per cent of those reporting identity theft to the US Federal Trade Commission (FTC) were unaware of the theft for more than five years. On average, 12 months elapsed between the date the identity theft occurred and when the victim discovered it. Not surprisingly, therefore, almost 80 per cent of the victims who report identity theft to the FTC do not know how or where the identity thief obtained their personal information.

The first indication of the theft may flow from a denial of credit to the victim due to a bad credit report caused by the actions of the identity thief. In some cases, the person who assumed the victim's identity may have committed crimes while using that identity. Thus, an innocent victim may find himself arrested for crimes he did not commit, or he may find himself saddled with an undeserved criminal record.

POOR BUSINESS SECURITY PROCEDURES

Of particular concern to organisations

is "business record identity theft." Identity thieves may steal records containing employees' or clients' personal information. The institutions can include hospitals, tax offices, municipalities and schools. In some cases, the records are stolen by insiders. This raises the question of corporate responsibility for the criminal acts of its employees, and whether corporations have adequate employee screening and data security measures to reduce the opportunity for identity theft to a minimum. Beyond the legal implications for corporations is the harm done by such thefts to relations with employees and clients.

The mechanics of identity theft range from the banal to the sophisticated. Only 17 percent of the consumers reporting identity theft to the FTC know how their identity was stolen. Of those who do know, almost 70 per cent say the source was an acquaintance or a stolen purse or wallet.

Speaking in April, the FTC's chairman, Timothy Muris, cited the case of a Seattle man who stole the identity of 400 individuals by sifting through garbage cans. On the other hand, Simson Garfinkel tells of a sophisticated identity theft ring in Detroit that used data from the computers of a Texas company where one of the thieves was employed. The company processed data for American Express credit card customers. The thieves used this information to produce counterfeit birth certificates, Social Security cards, drivers licences and automatic banking cards.

Just days after the September 11th attacks in the United States, the Privacy Rights Clearinghouse issued a warning that fraudsters would use this situation to contact consumers stating that company databases were damaged and that the caller needs critical information to reconstruct the accounts that were affected. Furthermore, hundreds of thousands of papers were scattered on the streets of Manhattan after the collapse of the World Trade Center towers. Some of those papers may have contained identifying information, including Social Security numbers, frequently used by investment companies as account numbers.

The actual theft of identity is only part of the story. The financial consequences to business and government can be substantial. Perhaps the most troubling aspect of identity theft is the lengthy trauma often endured by victims trying first to persuade authorities of the seriousness of their plight, then to restore their standing in the eyes of the financial and, sometimes, criminal justice communities. As delegates learned at the first National Conference of Privacy Activists, organised by *Privacy Journal* publisher Robert Ellis Smith in April, restoring one's creditworthiness and reputation may take years. Throughout that period, the victims themselves may be seen as criminals trying to deny responsibility for debts. And, inevitably, some individuals who have not been victims of identity theft will claim that they are, to avoid responsibility for debts they did themselves incur.

TECHNOLOGY IS NOT FAILSAFE

More secure identification systems (for example, photographs on credit cards) present a double-edged sword. They may help reduce identity theft in some situations. However, a thief might still manage to obtain a more "secure" form of identification in the victim's name - for example, by using stolen or forged "breeder" documents such as birth certificates to "authenticate" their assumed identity. It then becomes even more difficult for the victim to persuade financial institutions and government authorities that their supposedly "secure" identification has been hijacked.

Privacy Rights Clearinghouse Identity Theft Resources: www.privacyrights.org/identity.htm

US Senate Judiciary Committee hearings: www.judiciary.senate.gov/hearing.cfm?id=171

US General Accounting Office (GEO): www.gao.gov/new.items/d02363.pdf

Banks - beware of your online partners

Banking customers are increasingly conducting their financial transactions online. However, both they and the banks that serve them may be in for a shock with the growth of online financial fraud. In particular, banks must ensure that companies they may use to provide online services to customers do not become the weak link in the security chain.

The online news service CNET is carrying a series of articles on the increasing number of security breaches that occur as consumers move to online banking. Some of those breaches are occurring because banks may rely on website providers that do not have adequate security. Says the report: "Hackers often target hosting companies and ISPs, usually the weakest links in the chain, to bypass firewalls."

In April, a report by the US-based Computer Security Institute concluded that "the threat from computer crime and other information security breaches continues unabated and... the financial toll is mounting." As in previous years, the report noted, the most serious financial losses occurred through theft of proprietary information (26 respondents reported $170,827,000 in losses) and financial fraud (25 respondents reported $115,753,000).

For further information: http://news.com.com/2009-1017-891346.html and www.gocsi.com/press/20020407.html. See also "EU Forum Tackles Cybercrime" (PL&B Int Feb 2002 p.14-15.)