Stolen identities

Jennifer Whitson and Kevin D Haggerty argue that companies' zest for customer data and the huge growth in e-commerce is exacerbating the problem of identity theft.

The thwarting of identity theft preoccupies most modern institutions. And while identity theft is a criminal act, the most common responses to this crime fall outside of the legal system.

At the most general level, identity thieves manipulate someone's personal information to secure some benefit. They can acquire this data from dumpsters, customer service representatives, trojan horse computer programs and by stealing computers or hacking into corporate databases. Victimisation ranges from the single instance credit card fraud to more elaborate, extended uses of a person's documentary identity.

Commonly recognised as the most rapidly rising crime in both North America and the United Kingdom, the latest Home Office estimate is that identity theft costs the UK economy £1.7 billion per year, while in the United States, the Bureau of Justice Statistics estimate that in the second half of 2004, over 3.6 million households learned that they had been victims of identity theft (Bureau of Justice Statistics, 2006; Home Office Identity Fraud Steering Committee, 2006).

Identity theft is related to wider changes in communication systems. As commerce has become increasingly informational, it depends ever more on reliable data which is used to avoid risk and maximize profits. Pervasive identity theft can increase the costs of verifying data and dealing with customers. It also risks undermining the public trust in the informational systems which are the cornerstone of e-commerce. Attuned to these dangers, institutions have responded to identity theft in four different ways: (1) making data collection more secure (2) disseminating consumer protection information, (3) offering new services and products, and (4) changing institutional security practices and technologies.

Government, law enforcement and corporations compile and analyse data on instances of identity theft in order to predict future trends, educate the public and lobby for legal reforms. The information is also used in forms of 'dataveillance', as institutions try to pinpoint and prevent identity theft as it is occurring. To facilitate this data monitoring, institutions require access to more and more of a consumer's personal information. In the case of American Express, for example, this can include access to a client's credit report and highly codified data on their lifestyle and consumption patterns. Such information purportedly allows major financial institutions to differentiate in real time between legitimate and suspicious transactions. In a trend that mimics the increased use of profiling in criminal justice, private institutions use such data to subject consumers to heightened scrutiny on the basis of their relationship to statistical consumption profiles.

In a trend that mimics the increased use of profiling in criminal justice, private institutions use such data to subject consumers to heightened scrutiny on the basis of their relationship to statistical consumption profiles.

By simply carrying out routine daily activities, an individual also potentially exposes their personal data to identity thieves. Increasing awareness of these risks has pushed target hardening and 'responsibilisation initiatives' to the forefront of measures to counter identity theft. The specific measures that are advocated are constantly evolving, but some of the more familiar responsibilisation strategies involve encouraging individuals to keep personal information private. They are reminded to carry a minimum amount of credit cards and identifying information. Passwords should be added to bank accounts, credit cards and telephone accounts and these should be changed regularly. Consumers are encouraged to monitor their billing cycles and scrutinise bank and credit card statements as soon as they arrive. Creditors should be contacted immediately if bills are late or if documents contain errors. All items containing personal information should be stored in a safe (ideally locked) location. The iconic technology in this regard is the paper shredder. A generalised program of shredding is encouraged, encompassing receipts, copies of credit applications, insurance forms, medical statements, credit offers and magazine mailing stickers.

Such responsibilisation measures are augmented by anti-crime products and services such as safes, computer locks, firewalls and encryption software. Even household locks and alarms are being re-coded to foil identity thieves based on the awareness that burglars are now really seeking personal information. New services are marketed to reduce the impact of

Continued on next page

identity theft, including American Express's 'fraud protection guarantee' which ensures cardholders will not be liable for fraudulent charges or deductibles if victimized by identity thieves. Nonetheless, American Express still aggressively markets two types of insurance against identity theft, and cardholders are encouraged to purchase both to ensure maximum protection. Similar services are available from other financial companies, credit bureaus and insurance companies.

Responsibilisation efforts designed to reduce crime risks through personalised and market-based initiatives are often criticized for ignoring the social and institutional structures that facilitate crime. This is nowhere more apparent than in identity theft. Rather than identity theft being the result of the public being sloppy or irresponsible with their personal data, research suggests that most identity theft results from information lost through the careless data management practices of major institutions. More than 50 per cent of stolen identities involve thefts by employees or people impersonating employees. Other research has noted that up to 70 per cent of identity theft can be traced to leaks that occur within organizations (Collins and Hoffman, 2004: 6; Jewkes, 2002). While some companies are now attuned to the potential public relations nightmare that can result from lax data handling practices, the informational security of the major institutions that compile and hold vast quantities of the public's personal data have consistently been found to be wanting. Not only have these institutions been slow to respond to identity theft, but many have actively fought measures designed to reduce such crimes as they would necessitate costly upgrades to security technologies or practices that might harm their profit margin. This situation results in companies calculating the costs of upgrading security protocols versus the costs of not doing so, and occasionally gambling with their customer's private information (Sullivan, 2004).

Rather than contemplate measures to reduce our reliance on these proliferating informational identities, ever more detailed documentary identities are instead being entrenched, combined and triangulated to establish a person's true identity. Following this logic, personal information needs to be more detailed than in the past — an assumption that encourages the development of new forms of official documentation and further scrutiny of a person's informational profile. In the process informational security measures are poised to become more elaborate and intrusive as they simultaneously reproduce the institutional reliance on personal information that has ultimately made identity theft possible.

■

***Jennifer Whitson** is a PhD Candidate in the Department of Sociology and Anthropology at Carleton University, Canada.*

***Kevin D Haggerty** is Editor of The Canadian Journal of Sociology, Professor of Criminology and Sociology, University of Alberta, Canada.*

References

Bureau of Justice Statistics. (2006) 3.6 million U.S. households learned they were identity theft victims during a six-month period in 2004. http: //www.ojp.usdoj.gov/bjs/pub/press/it04pr.htm.

Collins, J. M., and Hoffman, S. K. (2004) *Identity theft victims' assistance guide: The process of healing*. New York: Looseleaf Law.
Home Office Identity Fraud Steering Committee. (2006) Identity theft: Don't become a victim. http: //www.identity-theft.org.uk/.

Jewkes, Y. (2002) Policing the net: Crime, regulation and surveillance in cyberspace. In Y. Jewkes (Ed.), *Dot.Cons: Crime, deviance and identity on the internet* (pp. 15-35). Cullompton: Willan.

Sullivan, B. (2004) *Your evil twin: Behind the identity theft epidemic*. New Jersey: Wiley.