ARRAY Logo

icon

Big Deal Identity Theft

By Martin Nemzow
Network Performance Institute
Miami, FL 33141
www.networkperf.com
mnemzow@networkperf.com

Mr. Nemzow has consulted in high-tech for 20 years, assisting several achieve IPO status. He has been active in marketing, commercial banking, insurance, and software development on personnel, strategy, financial, technology implementation, manufacturing, and day-to-day operational matters. As president of Network Performance, which is deploying a new paradigm for international currency translation and time-independent accounting, he holds several patents on those processes. He is the author of 20 McGraw-Hill books, including the bestselling McGraw-Hill books Web Video Complete and Ethernet Management Guide, 3rd Ed. online and top-selling ecommerce book, Building Cyberstores or construccion dé Ciberalmacenes. You also can read his ecommerce-business columns for WebServer Magazine online at http://webserver.cpg.com. For more information see http://www.networkperf.com/marty.htm.

Identity theft is the fastest growing crime in the United States; it is also the fastest growing crime in some other industrialized nations. Although the effects of this crime inconvenience the individual attacked but really cost the indemnifying credit card processors, the nature of this crime will change the business and banking landscape in a significant way. The most fundamental effect will be the extension of identity crime against banking and business organizations. That will be a big deal.

Look at the numbers. An identity theft against an individual results in an average loss to the individual of about $400 and hours spent denying debts and signatures, the credit card processors of about $13,000, and the police investigative units and court systems of about $1600 according to the FBI and the Economic Crime Task Force. It might be a major hassle for the consumer, but is represents a controllable risk for card issues and processors. Nevertheless, this still represents small risk and small crime.

It is only a matter of time before insiders and knowledgeable information processing professionals fake a known organization and an operating unit in order to divert an entire payroll payment, a quarterly tax payment, a treasury investment, or issuance of credit. The dollar values are astronomical; easily 10 to 35 million dollars, and perhaps even more. It is only a matter of imagination and the ability to sneak information into databases, create of new accounts and fake payment authorizations, and some simple social engineering to kite money from one place to another, and then another beyond the reach of reversal.

Imagine the diversion of product, payment for product, or intramural divisional fund transfers. That amount of money buys anonymity, security, and even a new nationality. I suspect the chance for recovery or restitution will be very low. Because the burden of the attack is against the officers of a legal entity,

the board of a corporation, or the duped operating people, personal vendettas are unlikely. This increases the chance of getting away with such a crime through government, legal, or alternative channels. Furthermore, like many past economic thefts and frauds, the victims are as unlikely to report or prosecute the crime. The nature of most legal systems, the lack of laws adequately defining theft, fraud, and diversion, and the insufficiency of uniform international cooperation prime the growth for corporate and banking identity theft.

The solution? While technology might help, and new prosecutorial venues, the reality is that people systems need to adapt. Authorization forms and countersignatures, IDs and passwords, and new tracks for oversight are the best courses of action. Forensic accounting and security measures will just detail the open doors and methods for accomplishing specific thefts; they will achieve nothing to prevent or minimize corporate identity thefts. Online banking, shared systems, ISP and ASP services, outsourcing, and other commercialization of IT services only extends the opportunity for new economic crimes. We will need to train employees at all levels not only to perform the rote jobs better but to understand the values and assets of the organization and how specifically to protect them. Identity theft is just a matter of time.