The John Liner Review

Vol. 18 No. 2
Summer 2004

Loss Control

Identity theft is proliferating. Business and consumers can take proactive steps to stem the tide.

Identity Theft: How Companies and Consumers Can Combat the Nightmare

CHRISTOPHER T. MARQUET

The first clue that Mari Frank had bills of about $50,000 came out of the blue. The California lawyer received a call from a Delaware bank, asking why she had not paid an $11,000 balance on a toy store's credit card.

Something was seriously wrong.

Frank had never obtained that credit card, much less incurred such high debt. It didn't take her long to realize she had become a victim of identity theft.

Identity Theft: Fastest Growing Crime in the United States

Identity theft occurs when someone assumes another individual's personal identity to establish credit and incur debt, take over financial accounts, apply for loans, rent housing, file for bankruptcy, or land a job. The impersonator can steal thousands of dollars in the victim's name without the victim realizing it for months or even years.

Attorneys, corporate executives, and other high-profile professionals are particularly vulnerable to identity theft because many of their vital statistics are a matter of public record. For example, last year, using information from a lawyers' directory, a prisoner already serving time for fraud stole the identities of 12 Boston lawyers. He obtained birth certificates and credit reports, opened new accounts, stole from exist-

ing ones, and netted hundreds of thousands of dollars to purchase luxury cars and apartments.

Identity Theft Is a Felony

A federal felony since 1998, identity theft that crosses state lines is punishable by up to 15 years in prison, a fine, and forfeiture of any personal property involved in the crime. Despite that threat, identity fraud is a burgeoning criminal enterprise. Police often are unresponsive to victim complaints because they choose to focus on other, more pressing, crimes. As a result, security experts view the identity theft as an almost-perfect crime.

Identity theft is neither new nor highly sophisticated, but in an increasingly cashless society it is an easy crime to commit.

In 1999, the Federal Trade Commission's (FTC) Identity Theft Data Clearing House responded to 23,000 calls reporting identity thefts. The agency estimated that nearly 10 million consumers were victimized in 2003, with the number expected to increase. This means that somebody is victimized by identity theft every three seconds!

Consequences For Victims Can Be Grave

According to a FTC survey, the average victim spends 30 hours and $500 cleaning up his or her credit record. In the meantime, victims can lose job opportunities; be refused loans for education, housing, and cars; or even be arrested for crimes they didn't commit — ranging from traffic infractions to felonies — because criminals give a victim's fake identification when arrested. Sometimes, victims even have to prove that they are victims, not deadbeats trying to get out of bad debts.

Identity Theft Is Easy to Accomplish

Identity theft is neither new nor highly sophisticated, but in an increasingly cashless society — along with the growth of the Internet, advanced technology, and easily available personal information — it is an easy crime to commit. All it takes is access to basic information such as a Social Security number; birth date; name and address; or driver's license, credit card, or bank account number — all of which can be easily obtained.

It's not necessary to pinch or find a wallet in order to steal an identity. Although computers provide identity thieves with a treasure trove of data, the identity criminal does not have to be a computer hacker with knowledge of "spying" software. The crook's stock in trade is the everyday transaction that generates basic identifying information from such common resources as retail sales and the files of doctors, accountants, lawyers, schools, and insurance companies. Criminally minded people working in these offices have easy access to clients' and staff members' personal data. Many identity crimes are committed by employees — the very people businesses entrust with such important information.

Some Recent Examples of Identity Theft Scams

According to the recent FTC survey, businesses and financial institutions lost some $47 billion and consumers lost nearly $5 billion in the past year because of such criminal acts. Consumer confidence in the security of online transactions has been seriously eroded in recent years. Some recent cases underscore how widespread and costly the crime has become.

- In January 2001, a Dallas man used six different Social Security numbers to open 108 lines of credit and incur charges of nearly $1 million.
- In July 2001, a New York state insurance customer service representative used confidential data to open new credit card accounts and purchase $100,000 worth of products online.
- In November 2002, a low-level employee of a Long Island software firm used company passwords to access a well-known credit bureau's database. He stole information from 30,000 credit reports, emptied bank accounts, opened fraudulent credit card accounts, and obtained false loans. The losses from this scam, not yet totaled, are expected to exceed $2.7 million.

Common Information-Gathering Techniques

Some common information-gathering techniques used by these criminals include:

- "dumpster diving," where the crook rummages through trash bins looking for personal data;
- "shoulder surfing," where the impersonator peeks over a person's shoulder at an automatic teller machine (ATM);
- stealing such mail as bank and credit card statements, preapproved credit offers, new checks, and tax information;
- filing a phony "change of address form" to divert an individual's mail;
- fraudulently obtaining a credit report by posing as a landlord, employer, or someone else who legitimately needs such information; and
- using personal information shared by the victim on the Internet.

Uses of Stolen Information

With such pickings, the identity thief can:

- open a new bank account and write bad checks in the victim's name;
- call the victim's credit card issuer to request a mailing address change, then run up huge charges on the account (of which the victim remains unaware because the statements are sent to a new address);
- open a new credit card account in the victim's name at a false address, resulting in a delinquent account that becomes a difficult-to-expunge part of the victim's credit report;
- create counterfeit checks or acquire debit cards and drain the victim's bank account;
- take out loans in the victim's name without making payments, damaging the credit record; and
- establish fraudulent cellular phone service.

Preventive Actions for Businesses

Businesses have a legal and moral responsibility to keep client and employee information secure. Vital company data should also be protected, with all divisions of the organization — e.g., information technology, customer service, compliance, human resources, legal — involved in the process. Risk managers must play a key role in protecting this sensitive data by taking the lead in the following actions.

- Conduct a "personal data protection audit" throughout the organization, paying close attention to human resources files and customer data files. Are policies and procedures adequate and, if so, are they being followed in practice?
- Perform comprehensive background checks on all employees, especially those with access to vital information about the company, customers, and staff, since many mass cases of identity fraud involve employees abusing the trust of their employers.
- Store all written information in secure and monitored file cabinets or file rooms, always using cross-cut shredders to dispose of confidential information.

Businesses have a legal and moral responsibility to keep client and employee information secure.

- Develop and enforce procedures for transmitting personal and confidential information, whether through faxes, e-mails, or other correspondence.
- Develop and enforce a written privacy policy and incorporate the policy into company by-laws, handbooks, and client information.
- Develop and maintain a secure encryption system for conducting online transactions and inquiries.
- Use and continually monitor the most effective and efficient firewall and antivirus software.
- Invest in a "privacy seal," which adds to consumer confidence and is especially important for e-commerce businesses.
- Invest in fraud detection software that identifies inconsistencies in transactions.

Preventive Actions for Consumers

Consumers can take the following preventive steps.

- Check credit reports from each of the three major bureaus at least annually.
- Cross-cut shred documents containing private or vital information — especially bank and credit card statements and preapproved credit card solicitations.
- Reduce the number of preapproved credit card offers, telemarketing, and spam by "opting out" with the credit bureaus (888-5-OPTOUT), Direct Marketing Association (www.dmaconsumers.org), and the FTC (www.donotcall.gov).
- Use secure and unique passwords on all accounts.
- Close or cancel unused credit cards. Sign credit cards with "Check ID" rather than signature.

When identity theft is suspected, the FTC recommends taking steps immediately

- Guard your Social Security number.
  * Never carry your Social Security card in your wallet, write the number on a check, or give the number to anyone unless absolutely necessary.
  * Check your health-care card identification number — it is usually your Social Security number. Request that it be changed or do not carry the card.
  * Make sure your driver's license number is not your Social Security number; if it is, change it at the Department of Motor Vehicles.
- Send mail through a U.S. Postal Service box, not a private mailbox.
- Be wary of telephone solicitors. Never reveal personal or financial information over the phone unless you have initiated the call.
- Examine all bank and credit card statements upon receipt, reporting inconsistencies or unknown charges immediately.
- Report any bills that don't arrive on time. They may have been stolen.
- Be vigilant of "shoulder surfers" when using ATM machines or eavesdroppers when on the phone.
- Download all antivirus and software updates.
- When shopping online, look for security tags on Web sites.

Actions To Take When Identity Theft Is Suspected

When identity theft is suspected, the FTC recommends taking the following steps immediately:

- Contact the fraud departments of each of the three major credit bureaus requesting that a "fraud alert" be placed in the file.
- Provide a written statement to creditors asking them to call before opening any new accounts or changing existing accounts.
- Close accounts believed to have been tampered with or opened fraudulently. Do not cancel all credit cards, but notify each credit grantor of valid accounts and request that they confirm address-change attempts before granting them.
- File a police report with local police and with the police in the community where the identity theft occurred. Be persistent if the police are reluctant to take or act on the report.
- Follow up all phone contacts in writing, using certified mail, return receipt requested.
- Keep copies of all reports, forms, and correspondence.
- File a complaint with the FTC. This agency provides victims with advice and additional resources.

Can Identity Theft Be Stopped? Not Entirely.

The repair process can be lengthy and complex, with victims feeling an overwhelming sense of powerlessness. While identity theft is a growing problem with serious consequences, individuals and companies can defend themselves by being vigilant, using common sense, and taking proactive steps to protect vital personal identifying information. The government has gotten into the action and begun to respond with legislation and more enforcement. With educated consumers, a proactive corporate world, and sensible government response, the tide can be stemmed on identity theft.

Christopher T. Marquet is executive managing director and founding principal of Citigate Global Intelligence, an international business intelligence, corporate investigation, and business controls and security consulting firm. He can be reached at *chris.marquet@citigateglobal.com*.