VOLUME 13 • ISSUE 5 • JULY/AUGUST 2006

BarNotes

A Publication of the San Fernando Valley Bar Association

Who Are You?

And More Importantly, Why Are You Claiming To Be Me?

Identity Theft Prevention is the Key to Protection

BY MICHAEL HACKMAN AND MOLLY BABCOCK-MARCUS

The client comes home from work, open the day's mail and find a credit card statement showing thousands of dollars in charges for items the client never purchased from places the client has never been. Someone out there knows the client's name, address, perhaps Social Security number, credit card information, and/or bank account numbers. Someone is posing as the client and running up outrageous bills, possibly committing crimes, and the client is going to be left with the financial, emotional and legal aftermath.

For an estimated 10 million Americans whose identities were pirated in 2004, it's very real. Victims of identity theft are likely to face long hours (and sometimes years) closing tarnished accounts and opening new ones, repairing credit records, and other-wise cleaning up the damage. They also may find themselves being denied loans, jobs and other opportunities because an identity thief ruined their credit and reputation.

Today assuming another's identity is astonishingly easy - so easy that the FBI and Interpol state that identity theft is the fastest growing crime throughout the world.

What is Identity Theft?

This broad term includes numerous privacy crimes, including theft of a Social Security number, the cloning of a credit card, debit card, or cell phone, or opening a new account. A Federal Trade Commission official gave a comprehensive definition, calling identity theft "stealing another person's name, address, Social Security number, or other identifying information in order to commit a crime."

One type of identity theft involves actually taking over an existing account. As a practical matter, account takeovers are less of a threat to a victim's finances than other types of identity theft because the harm is usually discovered when the victim receives the first monthly statement from the bank or credit card company and (if they review their statement carefully) the damage is limited to less than two months, and liability to no more than fifty dollars on a credit card.

More frightening to the consumer is the kind of identity theft that frequently cannot be detected until after the victim's credit has been severely damaged. It is known as "true name" fraud. The thief uses the victim's name to open a new bank account, obtain a new credit card or take out a loan for a big-ticket item. The thief re-routes the statements to a new but reasonable address to avoid tipping off the lenders and the accountholder. Victims of true name fraud are for a time oblivious to the theft because the monthly statements are going to another address.

According to Javelin Strategy & Research's *2005 Identity Fraud Survey Report*, address changes are among the top three fraud devices used by identity thieves, and account for almost 10 percent of successful fraud attempts. Victims usually discover the theft when they are turned down for a loan, or begin to receive calls from unknown creditors demanding payment for items they didn't purchase, or in some cases, are actually sued. FTC statistics (*National*

continued on page 16

Who are you, continued from page 14

and State Trends in Fraud & Identity Theft, January-December 2004) show the average time between the beginning of criminal activity and discovery is about fifteen months, which is enough time for a criminal to destroy the victim's credit and turn their life upside down.

In a third type of fraud, known as "identity cloning," the imposter uses the victim's information to establish a new life. He or she actually lives and works as the victim. Felons, undocumented immigrants, and people who do not want to be tracked favor this type of scheme. If the thief is arrested and provides a victim's personal information to law enforcement, the victim may have a criminal record or outstanding warrant without realizing it. According to one survey, clearing up the damage caused by identity cloning takes, on average, seven years, and often a victim never regains financial health.

Role of the Internet

The opportunities provided by the Internet have transformed many legitimate business activities, augmenting the speed and range with which transactions are conducted, while also lowering many of the costs. Consumers are banking, shopping, accessing their offices remotely, and engaging every type of online activity. They've grown accustomed to the digitalization that facilitates everyday transactions. Yet, along with its obvious economic benefits, the Internet has created enormous opportunities for economic offenders. As more information and transactions are undertaken in digital format, more sources of information are available for thieves to exploit. It has never been easier or more profitable for thieves to access and use personal information. Operating from the privacy of their home or office through the anonymity of the Internet, cyber-criminals enjoy minimal risk of detection. They have found an open range where they can exploit the carelessness, or weakness, or bad luck of others with virtually no one to stop them.

The Internet provides still another benefit for criminals. It allows them to steal personal information from databases anywhere in the world. As more companies outsource personal information, the opportunities for identity theft are greatly increased. When data is outsourced, it places personal information in the hands of third parties, often in countries where data protection laws are far less stringent than in the United States. Companies engaging in offshore outsourcing are willing to accept a certain amount of risk from identity theft with an offshore provider because of the cost benefit. "For these organizations, it amounts to a trade-off between due diligence and potential savings, but the growing trend in offshore outsourcing compounds the problem of identity theft," says Samir Kapuria, director of strategic solutions for Symantec.

Going for the Money

The U.S. Department of State (*International Information Programs, August, 2001*) has reported that organized crime is increasingly exploiting the opportunities afforded by the Internet. According to the report, the Internet and the growth of electronic commerce offer enormous prospects for illicit profits and new targets for infiltration by organized crime families. "The synergy between organized crime and the Internet is not only very natural but also one that is likely to flourish and develop even further in the future," says Phil Williams professor of International Security Studies, University of Pittsburgh. Criminals who steal and use other people's identities tend to be highly organized and work in teams. For them, it's a business, not an avocation. "Today's identity thief is not the lone gunman of the past," says Chris Painter head of the Computer Crimes Section of the Department of Justice, "Organized crime goes where the money is, and the cyber world is beckoning to them." Analyst Matt Ziemniak, with the National Cyber Forensics and Training Alliance referred to them as, the

Web Mob, "They are a type of crime family set up like the old mafia. They know each other only online, except those at the very top."

For felons on the run or for terrorists wanting to move freely in the country, obtaining someone's identity is the `gold standard.' They'll pay top dollar for it. To make matters worse, when personal information is downloaded on the Internet, it's easy to trade and sell in digital alleys and chat rooms all over the world. "When criminals can compile enough information about individual citizens to ring up thousands of dollars against their credit or bank cards, there is absolutely nothing to stop them from selling that information to terrorists, or foreign intelligence services," says Jim Hedger (*Identity theft On the Rise-Scarier Than Click Fraud, Insider Reports, August, 2005*).

Challenges for Attorneys

Conflicting procedural laws covering multiple jurisdictions are a significant challenge for attorneys working on identity theft cases. Even though California-style laws aimed at curbing identity theft have been enacted in several states, these laws are sufficiently different to make compliance across jurisdictions difficult at best, if not impossible. Traditionally, the question of jurisdiction has been settled by following geographic boundaries, but identity theft is a borderless crime, and geography is no longer a measure of jurisdiction.

A typical identity theft may involve a California victim, a thief residing in Washington, who commits fraudulent acts in Arizona and Oregon with credit cards issued through companies headquartered in Florida and Texas. For example, California identity theft statutes such as *Cal. Pen. Code § 530.8; Cal. Fin. Code. §§ 4022, 22470* and *Cal. Civ. Code § 1748.95*, that grant an identity theft victim the right to request and receive fraudulent account information from financial institutions and credit card issuers, are routinely ignored by businesses headquarter in states where the production of these documents requires a subpoena, even though the company has a nationwide presence.

Attorneys dealing with out-of-state businesses on identity theft issues are likely to find themselves researching jurisdictional questions while engaged full-time in writing letters and negotiating with lenders to prevent legal action. Some of the lenders/credit card issuers respond to letters within a couple of weeks. Others, mostly the larger banks and credit card issuers, do not respond at all. Dealing with these organizations is extremely difficult. Their phones are usually answered electronically and calls are transferred to company voicemail. Rarely are messages returned.

While the credit bureaus will usually remove fraudulent information on proof of identity theft, if the next data feed from the lender/credit card issuer contains the same erroneous information, the credit bureaus will report the inaccurate information again the following month. Attorneys are forced to follow up, sometimes for months, with the lenders/credit card issuers to ensure that they remove the inaccurate information they have provided to credit agencies and the credit bureaus.

Attorneys assisting identity theft clients should seek innovative solutions to confront the procedural and jurisdictional obstacles they are certain to encounter. To successfully deal with identity theft cases, attorneys must navigate layers of bureaucracy. The skill sets of the attorneys are a key determinant in getting identity theft issues resolved.

Michael Hackman *is a founding partner in the firm of Lewitt, Hackman, Shapiro, Marshall & Harlan in Encino, where his practice includes tax law, trusts and estate planning. He is a Certified Tax Law Specialist.* ***Molly Babcock-Marcus*** *is a litigation paralegal with the firm. The authors can be contacted at (818) 990-2120.*