

Beginning Monday, July 24th, ALL stories from the Nashville Business Journal print edition will be available online to print-edition subscribers ONLY. If you are already a print subscriber or you wish to subscribe, [click here to learn more.](#)

BUSINESS PULSE SURVEY: [Should HCA get the nod in Spring Hill?](#)

Identity theft: Knowledge is the best tool for protection

Nashville Business Journal - July 21, 2006 by [Mike Stuhle](#) Special to the Nashville Business Journal

[Print this Article](#) [Email this Article](#) [Reprints](#) [RSS Feeds](#) [★ Most Viewed](#) [★ Most Emailed](#)

With the Federal Trade Commission reporting the majority of Americans will become affected by identity theft within the next five years, it's easy to yearn for the old days, when identity thieves were limited to the people we knew - family, acquaintances and college roommates.

Now, our Social Security numbers reside on corporate databases instead of in our wallets and our personal information is fair game for everyone from insomniac hackers to sophisticated online scammers and organized crime. There's a subculture of people who commit the crime of assembling personal data and selling it on the Web.



Consider the increasingly sophisticated and creative "phishing" schemes, where millions of official-looking e-mails, ostensibly from your bank or even the IRS, are sent, soliciting information from the unsuspecting. Assuming they happen to get a 1 percent or 0.5 percent or 0.3 percent return they've still gained access to the personal information of hundreds and sometimes thousands of people.

According to Federal Trade Commission figures, there were 255,565 identity theft complaints made in 2005. Of those, 3,412 were in Tennessee. The largest percentage of those complaints were related to credit card fraud, followed by bank fraud, and phone or utilities fraud.

"People aren't really aware of the scope of the problem until they hear about the breach at the Veterans Administration or the laptop containing the personal information of thousands of investors being stolen from a brokerage firm," says Jeff Zander of Zander Insurance Group, which markets a reimbursement and credit restoration product for victims of ID theft. "But the fact is, your personal information is everywhere. You can shred your garbage, shred your bills and be the most paranoid person in the world, and you can still become a victim."

A common misconception is that identity theft is committed when your credit card is stolen and fraudulent charges are made. In fact, the Federal Trade Commission considers that credit card fraud. Identity theft occurs when individuals use your personal information and, for example, systematically establish credit in your name to defraud banks and loan companies.

Tim Amos, senior vice president and general counsel for the Tennessee Bankers Association, a 230-member trade association for banks in Tennessee, points out that his membership is now required by federal regulation to adopt a number of policies aimed at stopping increasingly sophisticated identity thieves. A bank's first defense is at the branch level, where they're now required to elicit sometimes multiple forms of proof of positive identification from potential customers and file a Suspicious Activity Report if that customer has any "irregular" transaction, creating a reporting burden on the bank and setting the stage for potential customer relations debacles.

Obviously, banks' largest concerns are fraudulent loans. "The loan process is, in and of itself, very involved in terms of checking on banking relationships, loan history, etc., and one would think that ID theft would be uncovered in the process, but the crooks are slick," Amos says. "They understand the process and have gone to great lengths to forge drivers' licenses and set up bogus accounts, maintaining them for a period of time, very much under the radar."

Identity thieves can be very careful to build a history, so in a lot of instances, the damage done to a victim is deep and pervasive, Amos says.

Once it happens and is discovered, the effort to fix it and discover the extent to which the victim's identity has been corrupted is a difficult and expensive proposition for the consumer and financial institutions that were pulled into the process.

While nearly half of ID theft is related to credit card, loan or bank fraud, employment related fraud - where a person uses a stolen Social Security number to get a job and receive benefits - is a growing concern. An increasing number of individuals are facing IRS audits because they didn't declare income that was fraudulently reported to their Social Security number.

Medical ID theft also is becoming more prevalent. And not only are individuals incurring debt associated with deductibles, co-pays and co-insurance from fraudulent claims, but they're grappling with the serious ramifications of having incorrect medical information reported to their insurance company.



Says Zander, "Usually people find out about ID theft when it's too late; when they're trying to buy a house, buy a car or refinance a house. They'll do something that triggers a credit search and find out they can't get approved."

According to Zander, the average amount of out of pocket cost a victim of identity theft will incur is \$1,800 for such expenses as legal fees, but it takes an average of 600 hours over three years to restore an identity.

Banks and insurance companies today are marketing products that provide various degrees of protection against the cost, but the bottom line is that the

burden of proof falls to the victim.

"When you call up a creditor and say, 'There's a \$7,000 bill and that wasn't me,' the first thing they're going to say is 'prove it.' There's a lot of diligent legwork that goes into that, and for most people, their biggest expense is lost wages as a result of that effort," says Zander.

As a minimalist approach, he recommends that individuals take full advantage of the Fair and Accurate Credit Transactions Act, which went into effect in 2005 and requires each of the three major credit bureaus to provide an individual with one free copy of their credit report each year. He suggests staggering your requests to once every four months - six times a year for a married couple.

The federal government's lead agency on the ID theft issue is the Federal Trade Commission. The FTC has a special Internet site dedicated to the steps you can take to protect yourself from identity theft and what to do if you become a victim: www.consumer.gov/idtheft/index.html.

In addition, a half dozen federal agencies have banded together to jointly support the Internet site www.onguardonline.gov, which provides tips from the government and technology industry about guarding against Internet fraud and protecting personal information.

Mike Stuhle is a Nashville-area freelance writer.