

---

# FEATURE ARTICLE

---

## **For More Information Contact:**

Mindy Lally  
314.983.1288 or 314.983.1200  
[mlally@bswllc.com](mailto:mlally@bswllc.com)

Danielle Oser  
314.983.1266 or 314.983.1200  
[doser@bswllc.com](mailto:doser@bswllc.com)

February 15, 2006

## **For Immediate Publication**

### **Foiling Identity Thieves Takes Vigilance, Persistence**

By Don Mitchell, CPA, CFE

As most everyone now knows, an identity thief is someone who gets and exploits another person's or organization's financial data. He or she may steal Social Security, credit card, banking or other confidential information to tap existing accounts, or open and charge up new ones.

How big a problem is identity theft? According to a 2003 Federal Trade Commission (FTC) report, 27.3 million Americans have been victims of identity theft in the last five years, including 9.9 million people in the last year alone. The average loss was \$4,800, with the total cost approaching \$50 billion annually. Individuals spent close to 300 million hours resolving problems resulting from the crime. So it's well worth the effort to avoid becoming a victim.

#### **Where Thieves Lurk**

An identity thief may steal your purse or wallet to get credit cards and IDs, but today's criminals are often more resourceful. You could encounter them in:

*Public places.* Thieves may peer over your shoulder or eavesdrop to get account numbers, personal identification numbers and passwords. Beware at store checkouts, phone booths and automated teller machines.

*Phone.* Rip-off artists posing as telemarketers are after personal information such as your date of birth or Social Security number.

*Mailbox.* Identity thieves may steal credit card statements and pre-approved credit applications, using or activating them without your knowledge.

*Computer.* These scamsters hack into your home or business computer network and steal files. Or, they send spam e-mail to obtain personal information in exchange for a product

## **Foiling Identity Thieves Takes Vigilance, Persistence**

Page 2 of 4

or service they never intend to deliver.

*Front door.* Brazen con artists pretending to be salesmen could show up at your home or business, trying to finagle information.

*Trash.* Thieves dig through even the smelliest garbage for private information and records such as bank statements, credit card receipts and pre-approved applications.

These thefts aren't always obvious - smarter criminals know how to cover their tracks. For instance, they may have your subsequent credit card or bank statements sent to another address. By the time you learn of the unauthorized activity, they've depleted your accounts, run up big bills and ruined your credit rating.

### **How to Protect Yourself**

To avoid becoming a victim, heed the old warning: Don't talk to strangers. Shield your private information from people or organizations you don't know. Some information to closely guard includes your name, family maiden names, address, birth date, Social Security or other identification numbers, employer, income status, financial assets and account records, and health records.

Take special care in handling personal documents, such as your Social Security card, driver's license, birth certificate and passport. Keep track of what identification and credit cards you carry, and leave what you don't need at home. File away receipts and records, or shred them thoroughly before tossing them out.

Even the most careful person may still get hit. But you'll minimize the impact if you swiftly smell a rat and take action. So monitor all financial statements, immediately investigate red flags such as collection agency calls, and get and review your credit report annually.

### **What to do about Cybercrime**

Identity thieves love the Internet and e-mail, and they target both personal and business computer networks. To protect your systems from cybercrime, apply these safeguards:

*Password-protect systems.* Limit system access by requiring all authorized users to create an obscure password combination of numbers as well as upper- and lower-case letters, and change it periodically.

*Install a firewall.* Block unauthorized access by installing firewalls at key network connection points, such as the Internet, or customer or supplier local area network.

*Encrypt data.* As an added measure of protection, consider encrypting system data.

## Foiling Identity Thieves Takes Vigilance, Persistence

Page 3 of 4

This will help protect your system should an especially clever hacker manage to break through your firewall.

*Avoid file sharing.* Consider disabling system file-sharing features to prevent other computers on the Internet or from other networks from reading your personal or business files.

*Monitor activity.* Watch for suspicious activity by regularly reviewing system data logs.

*Stay a step ahead.* Periodically review and update your system's security to ensure you're taking advantage of the latest practices.

### **When You've Fallen Victim**

If, despite your best vigilance, you become an identity theft victim, follow these three steps to restore your identity and rebuild your credit:

1. *Notify the authorities.* Immediately report the fraud to one of the three major credit bureaus: Equifax (800.685.1111), Experian (888.397.3742) or TransUnion (800.916.8800). The bureau you contact will alert the others. They'll also place a fraud alert on your credit file, which instructs creditors to contact you before opening a new account or processing account changes.

In addition, file a report with your local police as well as a complaint with the FTC, which aids law enforcement agencies in identity theft investigations. If you think someone is using or may use your Social Security number, driver's license or passport, get in touch with the United States Social Security Administration (800.772.1213), United States Department of State Passport Services (877.487.2778) and your state's Department of Motor Vehicles.

2. *Prevent further damage.* Close all suspect credit or bank accounts. Ask the financial institutions to help you follow up with a written "ID Theft Affidavit." Developed by the FTC in collaboration with banking, credit and consumer advocates, this is a simple, universally accepted way to report fraudulent claims to credit issuers, banks and other financial institutions.

3. *Document everything.* Contact the three credit bureaus and order copies of your credit reports for your records. The bureaus should provide them at no charge. Request a letter from each bureau, and a police report, as proof of the crime and pending investigation. You can show this to your creditors and other institutions. Maintain all documents, including detailed notes and dates of related phone discussions, for later reference.

If you have trouble convincing creditors or agencies that you've been victimized by identity theft, you may obtain legal assistance to help ensure you're treated in accordance with

the Fair Credit Reporting Act.

**Why Vigilance Pays Off**

Identity theft hits hard. You stand to lose precious assets and your hard-earned financial reputation. Worse yet, you can spend countless hours getting out of the mess. By taking a defensive posture, you can help fend off would-be thieves. And if you know what to do when fraudsters strike, you'll be forearmed to restore your identity.

Don Mitchell, CPA, CFE is a Member at Brown Smith Wallace. He has more than 30 years of public accounting experience. As a Certified Fraud Examiner, he is specially trained to gather evidence, take statements, write reports, and assist in investigating fraud. Mitchell can be reached at 314.983.1248 or email [dmitchell@bswllc.com](mailto:dmitchell@bswllc.com).

Brown Smith Wallace is the second-largest locally owned independent full-service CPA and business consulting firm in Missouri with nearly 150 employees throughout the Midwest. Through a network of offices in St. Louis, St. Charles and Chicago, Brown Smith Wallace is the only CPA and business consulting firm that makes A Measurable Difference™ to its clients through the execution of its six measurable differences and by putting its guarantee in writing. For more information visit [www.bswllc.com](http://www.bswllc.com) or call 314.983.1288.

###

**EDITORS NOTE:** Permission to reprint is hereby given to all print, broadcast and electronic media. Permission is also granted for reasonable editing, including article title change and customizing for your audience/industry. **Please send a copy of the published information to: Brown Smith Wallace, Mindy Lally, 1050 N. Lindbergh Blvd., St. Louis, MO 63132**