

Identity Theft-Surviving the Crime of the Century

by Mike Tingle

When the long arm of the law finally caught up with the notorious bank robber Willie Sutton, they asked him, "Willie, why did you do it? Why'd you rob all those banks?"

Understandably, not a man with the greatest respect for police reasoning, Willie answered in amazement, "I rob banks because that's where the money is."

Well, compared to today's larceny rich feed trough of identity theft, Willie Sutton thrived on a diet of water and SlimFast-hold the SlimFast.

Willie's banks were brick structures, usually two-story affairs that had a sign out front that read, "Bank," which of course in the language of robberese flawlessly translated to, "Hayseeds, hit the dirt! Robbers, please step to the front of the line."



Today's banks are not so well marked, but they are virtually everywhere. Last year, ordinary Americans-the modern-day robber's First National Bank-lost over \$53 billion dollars to identity thieves, and not once did anyone report hearing the trademark yowl, "Stick-em up!"

Run of the mill identity thieves are still low-tech, principally your garden-variety Dumpster-divers looking for blank checks, credit card receipts and bank statements, which can be easily negotiated on the streets for drugs or chump change.

However, most identity thieves have gone high-tech. Consider the following.

- Image scanners and readily available blank paper check stock have made the once common, now increasingly rare cashier's check a throwback to the days of Willie Sutton. Deposit a cashier's check nowadays, and expect to wait at least ten days for it to clear.
- Digital camera phones have brought the lofty crooked art of shoulder surfing, which is the stealing of credit card numbers at checkout counters, to the common thief. Anyone, not just those scofflaws with Mensa memories, can steal a credit card number with a camera phone.
- Using identity theft to gain employment, and posing as an attorney, a convicted felon became the chief benefits officer of the \$11 billion, 200,000-person, Indiana pension fund.
- A man in the Midwest, wearing a cable company uniform, driving a cable company truck, quite successfully sold, installed, and billed for pirated cable service. Embarrassingly for the industry, his customers considered his service superior.
- Corporate intelligence officers (a/k/a corporate spies) incredulously but legally pay kitchen helpers up to \$200 per soiled paper napkin retrieved from the trash at America's superpower bistros just to see what might have been written on them.
- Paper shredded by cross-cut and ribbon-cut office shredders can now be reassembled almost as fast as it is shredded with the aid of scanning software that restores the image like puzzle pieces.

While it is true the laws are starting to catch up to the crime, it is still one of those light-years to Andromeda journeys. On April 14, 2004, the enforcement phase of HIPAA, the "Health Insurance Portability and Accountability Act" is finally law, only six (light?) years and \$100 billion in losses since passage.

The official maximum penalty for unauthorized release of medical records is a 10-year prison sentence and \$250,000 in fines. However, here is a piece of good advice; don't hold your breath for the Court TV premier of United States vs. Dr. Sawbones. HIPAA is so horribly riddled with question marks, a paralegal with a degree from the Captain Joe Hazelwood School of Law could build St. Elsewhere inside HIPAA's Swiss cavities with room to spare.

GLBA, the Gramm-Leach-Bliley Act is the fiduciary cousin of HIPAA. However, unlike HIPAA, GLBA is more than an Attorney's Relief Act. With nearly 10 million identity fraud victims in 2003, GLBA has wide support by both financial institutions and consumers. However, the question remains, with that many victims, is the law sufficiently toothy?

With so much personal data available to those who'd misuse it, how do we protect ourselves? Here are a few simple tips.

- Don't use easily decrypted passwords, like anniversaries, birthdates or pet's name, and change your passwords frequently. Commit passwords to memory and keep a written list in a safe deposit box at your bank, not at home.
- If your bank and credit card companies offer the service, check your account activity online daily.
- Shred anything that has individually identifiable information on it. The most innocuous information can sink your financial boat. If you don't use a professional shredding service already, find a drop-off center or a ship-in shredding service.
- Pay bills online. If you must write checks, take them to the post office. Never leave live checks in a mailbox. Thieves will steal them, "scrub-off" the amount and payee, and forge a new amount to them.
- Never release sensitive information over the telephone or email unless you have initiated the communication. Spoofers will pretend to be your bank, credit card company, etc.
- Never carry your social security number on your person.
- Have new checks delivered to your bank instead of your home and pick them up there.
- Late mail may be a clue that impersonators have stolen your identity. Call your financial institutions immediately. Credit card thieves may have changed your address without your knowledge.
- Another clue that you have been "taken" is if you are denied employment or a lease for no apparent reason. Check your credit report once a year.
- If possible, avoid using debit cards. Credit cards provide greater protection.
- Avoid using your mother's "real" maiden name to authenticate your identity. Instead, use an alias.
- Include this phrase with your signature on your credit cards, "photo ID required."
- Don't let greed cloud your judgment. Scammers use fabulous but phony inducements to lure their prey.
- Keep these numbers handy should you fall victim to identity theft: Federal Trade Commission: (877) ID-THEFT. Equifax: (800) 685-1111 TransUnion: (800) 680-7289 Experian: (888) 397-3742

It's generally believed in law enforcement that one out of three Americans will fall victim to ID theft in their lifetime. However, with nearly 10 million victims reported in 2003 alone, and nearly 28 million victims in just the last five years, the experts might be underestimating the crime.

Last piece of advice: with not much updating, your grandmother's warnings are still valid. Never talk to strangers. And, if it seems too good to be true, it probably isn't.

Novelist and screenwriter MIKE TINGLE lives in the Rocky Mountains with his wife and daughters. His works range from nonfiction to supernatural, horror, suspense, and thriller. He has also written numerous short stories and occasionally still freelances as a business writer and speechwriter, specializing on various aspects of the document destruction industry.