

## Top 10 Identity Theft Tips for 2008

### 1. Beware the Word "Prevent"

No person and no product can prevent identity theft. As long as criminals can benefit from stealing, there will be theft. Sensitive personal information (SPI) is everywhere, housed and archived in a mind-boggling variety of ways. Individuals and companies can reduce access to SPI and improve safeguards around it by working to change how we share, collect, store and dispose of information.

### 2. There Are No Guarantees

This mantra holds true for a lot of things in life and dealing with identity theft is no exception. While a number of instances of fraud can be restored to pre-theft status, some identity dilemmas simply can't be fixed. If you're on the 'no fly list' thanks to an imposter or an error, you'll stay there. A third-party solution cannot deliver a remedy.

### 3. Watch for "Shoulder Surfers" and "Skimmers"

Shield the entry of personal identification numbers (PINs), and be aware of people standing entirely too close by when using your credit or debit card in public. Especially with the advent of cell phone cameras, a sneaky, shoulder surfing thief can get your private information pretty easily, if you're not careful. It's also advisable to use teller machines that are familiar to you, so you are in a better position to identify when the equipment looks different or doesn't "feel right." Your increased awareness may reveal a skimmer's attempt to steal PINs and banking details at that site.

### 4. Keep Your Social Security Card Safe at Home

Unless you're on your way to fill out a job application, there are very few reasons to carry around the crown jewel of SPI. At lunch a few weeks ago, the woman beside me opened her wallet for a credit card and there was her Social Security card, too. Remember, ID theft and fraud are not exclusively credit-related – thieves can use a clean Social Security number to construct a whole new life.

**Additional note from Dave:** I regularly receive emails from Fight Identity Theft visitors explaining how they just had their purse or wallet stolen with their Social Security card inside. Remove that card today!

### 5. Destroy Before You Dump That Old Computer

Erasing data just enables the computer to write over that space again; it doesn't actually eliminate the original bits and bytes. Physically remove the hard-drive to ensure you're not tossing out or passing along your personal details. Our company is often called upon to recover data from an erased or damaged drive; we're very good at it – and so are some professional thieves.

**Additional note from Dave:** You could also consider using a software tool like Eraser to do a complete wipe of your drive. If you physically remove your drive, smash the drive with a hammer (find someone strong) before throwing it in the trash.

## **6. Choose "Forget Me" Instead of "Remember Me"**

How many Web sites do you frequent that invite you to enable an automatic log on the next time you visit? Don't check that box! When convenience trumps confidentiality, you're asking for trouble. The harder you make it for hackers to follow your trail into an online store or bank account, the better.

**Additional note from Dave:** This is absolutely necessary when using public computers. In fact, you should avoid accessing any secure sites from a public computer (like a library, internet cafe) or when using a public wireless network or wifi hotspot.

## **7. Don't Rely On Fraud Alerts Or Credit Freezes Alone**

Fraud alerts are meant to stop an identity thief from opening new accounts in your name. Credit freezes let you restrict access to your credit report, which would also make it hard for someone else to open new accounts. But, neither one will stop a thief from trading your SPI for cash, or using it for tax fraud or in any of the countless other ways fraudsters exploit stolen identities.

## **8. Practice Prudent Posting**

Social networking sites on the internet enable individuals around the world to chat, share photos, recruit employees, date, post resumes, auction property, and more. Because the Web makes it possible for any posted document to link with another, any data you put out online have the potential to stay there for what amounts to electronic eternity.

**Additional note from Dave:** I suggest creating usernames or an email address that don't contain your name or anything traceable to you, whenever possible. You also might consider using different usernames on different sites. This makes sense because if someone is able to determine that you use "CatLuvr55" on one site, it's an easy search to track down "CatLuvr55" on any other sites where you have a profile.

## **9. Keep That Key**

When you check out of a hotel where you were issued a card-key to unlock the door to your room, don't leave the card-key behind. Hold on to it until you're safely home and can shred or otherwise discard it safely. Some say it's an urban myth that the card-keys hold vital details like credit card numbers, while others report having tested and confirmed the presence of private data coded into the magnetic strip. Even if there's no definitive answer, why risk it?

**Additional note from Dave:** Not sure I'm convinced on this one. I'd need to see more data showing that it is a problem. Snopes.com debunks this pretty thoroughly.

## **10. What's In Your Wallet?**

Make photocopies of the personal material in your wallet: Driver's license, credit cards, insurance cards, all of it – front and back. Should your wallet be lost or stolen, you won't be left wondering what was actually taken, and you'll be able to quickly notify the appropriate agencies about what has taken place.