Combating Identity Theft: Beyond the Basics

Identity thieves are more sophisticated than ever. We've all heard the horror stories. But, how can we protect ourselves (really)?

Here are ten additional things you might want to do to help protect yourself from becoming the next victim of identity theft (and how to prevent victimizing someone else):

1. Never e-mail your (or anyone else's) personally identifying information unless you know the transmission is secure. If you don't know whether your e-mail (or a web site) is secure, don't provide your "personally identifying information" – that is, information that uniquely identifies you (or anyone else) and includes, but is not limited to: Full names, dates of birth, places of birth, credit card numbers, Social Security numbers, driver's license numbers, medical ID numbers and the like. Know, too, that pieces of information - such as your city and county of residence, age, gender, race, school name, job position, etc. - may be combined with other personal information to uniquely identify you. Keep private what should be private information about yourself and others!

2. Sign up for the National Do Not Call Registry, if you haven't done so already. The National Do Not Call Registry is managed by the Federal Trade Commission, the nation's consumer protection agency, and gives you the opportunity to limit the telemarketing calls you receive. Register your home telephone number and all of your personal cell phone numbers (and those of your children). Telephone numbers placed on the National Do Not Call Registry will remain on it permanently due to the Do-Not-Call Improvement Act of 2007, which became law in February 2008. NOTE: If your phone number(s) change, be sure to register your new number(s) as well. For more information, contact www.donotcall.gov or (888) 382-1222.

3. Keep a list or photocopy of the entire contents of your wallet (front and back) in a secure place (which is not your wallet or purse). WARNING: Copiers now have memory similar to your computer, cell phone and digital camera. The copier's memory may be keeping a record of your photocopied document. If you don't own the intended copier, make a list of all account numbers, expiration dates, security codes (the three or four digit number on the back - or front - of your credit card), along with the customer service and fraud department phone numbers. If you *do* own the copier, be sure to destroy the memory before donating or recycling it.

4. Reduce the number of credit and debit cards you carry with you.

5. Do not carry your Social Security card in your wallet or purse, except for situations when it is or may be required (for example, on the first day of a new job).

6. Always protect your Social Security number! Release it only when absolutely necessary, which should be rare. If someone (like your healthcare provider) asks you for your Social Security number on an intake form, for example, skip it and bets are no one will even notice. If they do, ask if another number can be used instead. If not, ask why they need your Social Security number (especially in light of already requiring your health insurance group and/or subscriber number). Most of the time, they won't know (which, more often than not, is for collection purposes). Ask further how it will be used and what will be done with it after it is used, and ask (for fun if nothing else) what would happen if you refuse to provide it.

7. Do not say (or allow anyone else to say) your Social Security number, or credit or debit card number out loud in a public place. In situations where you have provided your number, the person you gave it to may request to read it back to you (to verify its accuracy). Refuse. Instead, offer to repeat it to them. You know where you are and whether your location is secure. Can you say the same for the other person?

8. At least monthly, carefully review your credit card, bank and phone statements for unauthorized use. We know. It's a pain. Do it (regularly) anyway.

9. Request a free copy of your credit report once a year. The Fair Credit Reporting Act guarantees you access to your credit report for free from each of the three nationwide credit reporting companies - Experian, Equifax, and TransUnion - every 12 months. Unless you are in the market for credit or you are a victim of (or suspect) identity theft, you may want to stagger your requests so you receive one report every four months. That way, you can monitor your credit report on an ongoing basis without charge. For more information, visit the Federal Trade Commission web site at: http://www.ftc.gov/freereports

10. Two final words . . . passwords and PINs. When creating passwords and PINs (personal identification numbers), do not use the last four digits of your Social Security number, your mother's maiden name, your birth date and the like. Do not use consecutive numbers either (such as 1-2-3-4). Instead, use a combination of numbers, upper and lower case letters and symbols - at least eight characters long. And, be sure to (regularly) change your passwords. All of them. Again, we know. It's a pain. Do it anyway.

How best to protect your identity is ultimately up to you. Limiting who knows your personally identifying information (including friends and family) is a good start. If disclosure is required, know who is going to use your information and why, and how it will be protected and disposed of (properly).