

Identity Theft— It's No Urban Legend



U.S. Air Force art by MSgt. Joseph Stephenson



This seemingly happy ATM customer may not be smiling as much if he walks off without taking his receipt.

A Navy retiree found out someone had stolen his personal information and had established credit in his name when he received a phone call from a clerk at American Express. “Someone’s trying to cash a \$9,000 check in your name, made out to a Muslim or Arabic-sounding name,” she said.

The clerk had become suspicious because the address she had on file for the retiree didn’t match the address on the check. Investigation revealed that a lawyer had stolen the retiree’s identity.

The lawyer had a laptop computer with a list of several thousand military names, Social Security numbers, and other information. The common link among veterans on this list was that they had followed the once standard advice everyone received upon leaving active duty. They had filed their DD-214s with local county courthouses so they always could get a certified copy if necessary.

The problem with this system is that all documents filed at county courthouses become

public records. So, it should come as no surprise that separating veterans today are urged to invest in safe-deposit boxes.

Identity theft is one of the fastest growing crimes in America today. The Federal Trade Commission reported 600,000 to 700,000 cases in 2000. According to the FTC, many victims don’t find out their personal information has been stolen until they try to buy a house or apply for a loan.

There are many different ways this crime—a felony under federal law—is perpetrated. A thief may open a credit-card account, using your name, date of birth, and Social Security number. The thief then runs up a big balance and just ignores billings, which leads to the delinquent account being noted on your credit report. Another example is when a thief counterfeits your checks or debit card and drains your bank account.

Victims of identify theft face a long and difficult process to clean up the resulting mess. Here are some steps you can take to minimize the risk of becoming a victim:

- Annually obtain copies of personal credit reports to make sure they are accurate. Credit-reporting agencies will send fraud victims a free copy. When filling out loan or credit applications, ask how the company stores and disposes of the forms. Avoid companies that don't give satisfactory answers. Ask your employer how personal information is stored and who has access to it.

- Use only the initial of your first name and full last name on personal checks, which prevents criminals from knowing how the checks are signed. Use a work phone number instead of your home number on the checks. Don't include a Social Security number on your checks. Don't have new checks mailed to your home address; pick them up at the bank. Be careful with businesses using special check scanners that withdraw the amount of a purchase directly from your account. Be sure retailers are reputable.

- Protect all mail with sensitive information, such as credit-card bills, by placing it directly in a U.S. mailbox. Thieves easily can steal items from your home mailbox. Register with the Direct Marketing Association's mail preference service to reduce the amount of unsolicited offers you receive in the mail. Opt out of direct-mail marketing, e-mail marketing and telemarketing solicitations from companies that abide by DMA's services. Visit their website at www.thedma.org. Consider using a post office box. If no mail has been received for a few days, contact the post office to find out if a change-of-address form has been filed in your name. If mail is being diverted, notify postal officials. Do not put your Social Security number on your resume if you plan to send it by e-mail or regular mail.

- Photocopy the contents of your wallet, including 800 numbers to call if credit cards are stolen. Don't carry a birth certificate, Social Security card, or passport; leave them at home in a safe place. Keep the number of credit cards you carry to a minimum—preferably only one or two. That way, if you are victimized, there are fewer credit sources to contact. Close all credit accounts that you don't use. Protect your bank and credit accounts with passwords; memorize the passwords—never carry copies. When paying

with a credit card, scratch the account number off the receipt when signing it. Because the purchase already is approved, the business no longer needs the number. Shred all paperwork, including receipts that have account numbers printed on them. Never throw account numbers in the trash.

- Be careful about giving anyone personal information, such as Social Security number, date of birth, home address, or bank-account number. Never reveal this information to people over the phone unless you have placed the call to a source you trust. Ask for password protection for all telephone accounts. If someone calls you with an offer that sounds too good to be true, and they just need your personal information to confirm the prize, hang up the phone.

- Don't throw away old bank statements or other sensitive documents without tearing them up, shredding them, or otherwise blacking out the sensitive information. Follow this advice, too, when you receive pre-approved credit-card offers in the mail. It's perfectly legal for people to dig through trash left on the curb and to read or take your discarded mail and other property.

- Don't keep ATM personal-identification numbers in your purse or wallet. Never leave an ATM receipt at the machine because it contains account information.

- When ordering over the Internet, make sure the server is secure to prevent third parties from tapping your information.

- Be careful when dialing 800, 888, 877, or 900 telephone numbers. Such calls result in the company capturing your name, address, and phone number, which become part of an electronic profile.

- Review your monthly credit-card and bank statements for unauthorized transactions. Immediately notify the credit-card company or bank of any problems.

- Ask to have a special identification number put on your driver's license, instead of your Social Security number. ■

For more information about identify theft, contact the Federal Trade Commission toll-free at (877) 382-4357, or access them at www.ftc.gov.