

## Ten Simple Things You Can Do to Fight Fraud

- 1) **Protect your Social Security number, credit card and debit card numbers, PINs (personal identification numbers), passwords and other personal information.** A thief can use these details to order checks or credit cards, apply for loans or otherwise commit fraud using *your* name.

Among the preventive measures you can take: Don't provide financial and other personal information in response to an unsolicited phone call, fax, letter or email—it could be from a fraud artist masquerading as a legitimate business person or government official. Be particularly cautious with your Social Security number (SSN). While your employer and financial institutions will need your SSN for tax purposes, you have the right to refuse requests for your SSN from merchants and service providers (who have other ways to identify you.)

Keep bank and credit card statements, tax returns, checks and other sensitive documents in a safe place at home. Shred these documents before discarding them.

Also choose PINs and passwords for your bank and Internet accounts that will be tough for someone else to figure out. Don't use our birth date or home address, for example.

- 2) **Deal only with legitimate, reputable businesses.** Try to do business with companies you already know or that have been recommended. Do your research before giving money or personal information to an unfamiliar merchant (or charity or any other organization.)
- 3) **Get key details in writing and thoroughly check them out before agreeing to anything.** Don't rely on a sales person's oral representations for a significant purchase or investment. Get as much written information as possible, including a contract, specifying cost information and your consumer rights. If a marketer refuses to supply written information or employs high-pressure sales tactics to get you to act fast, take that as your cue to say "goodbye."
- 4) **Beware of "deals" requiring money up-front.** "Congratulations, you've won a free vacation!" "Get rich quick—at no risk!" "We'll fix your credit problems—fast." Do these sound familiar? They're likely to be schemes to trick you into sending money or providing bank account information in exchange for promises of goods

or services that will never be delivered. Be skeptical of any offer that's "free" or otherwise hard to believe and that, as a precondition, requires you to pay money (perhaps for a supposed "fee" or "tax").

- 5) **Be extra careful when providing personal information over the telephone or Internet.** Scam artists hide at the other end of the phone line or computer screen. So, don't give bank account information, Social Security numbers or personal data in response to an unsolicited phone call or e-mail. Remember that a legitimate company would never ask for passwords or other personal information by e-mail. Before providing credit card or other information to a Web site, confirm that the site is legitimate, not a copycat designed by a crook, by verifying that the Web site's address is an exact match for what appears in literature from the company or some other reliable source. You'd be wise to avoid an online merchant that doesn't list a phone number or physical address—possible signs that the Web site and its owners are fraudulent. Also look for assurances on the Web site about security procedures for safely transmitting and storing your credit card number, password and other personal information you're asked to provide.
- 6) **Safeguard your incoming and outgoing mail.** It could include checks, credit card applications, bank statements and other items of value to a thief. Try to send and receive mail using locked mailboxes or otherwise secure locations. Remove incoming mail from your mailbox as soon as possible. If your mailbox is unlocked and you're going to be away on vacation or some other travel, have your mail held at the post office or picked up by a neighbor. If you're expecting a check, a credit card or bank account information and it doesn't arrive in a reasonable period, notify the sender. As for outgoing mail containing a check or other personal financial information, put it in a blue Postal Service mailbox, hand it to a mail carrier or take it to the post office.
- 7) **Stop bandits from recycling your trash into cash.** Thieves known as "dumpster divers" pick through garbage looking for credit card applications, monthly bank statements, receipts, "loan checks" (mailed by financial institutions with offers to "write yourself a loan") and other documents they can use to commit fraud. Before tossing out these items, destroy them, preferably using a "crosscut" shredder that turns paper into confetti. Before selling, donating or disposing of an old personal computer, use special software to completely erase files that contain financial records, tax returns and other personal information. Also, "Be aware that thieves can sometimes access personal information from computer disks, even if you've deleted or revised the files on the disk," warns an FDIC Community Affairs Officer. "The easiest solution is to break any disk before throwing it away."
- 8) **Limit the confidential information in your wallet in case it gets lost or stolen.** Don't carry around more checks, credit cards or other bank items than you need. Consider reducing the number of credit cards you carry by canceling ones you don't use. Keep passports, Social Security cards and birth certificates in a secure place, not in your wallet. Never keep passwords or PINs on or near your checkbook, credit card, ATM card or debit card.

- 9) **Review your credit card bills and bank statements as soon as they arrive.** If you notice something suspicious, perhaps a credit card purchase you didn't make or an unauthorized withdrawal from your checking account, contact your financial institution immediately. While federal and state laws limit your losses if you're victimized by a financial fraud, sometimes your maximum liability depends on how quickly you report the problem. Also make sure you get your statement every month. If no statement arrives, that could be a sign that an identity thief has changed your mailing address for purposes of committing fraud in your name but from another location.
- 10) **Monitor your credit report for warning signs of fraud.** Most experts say you should check your credit report at least once a year from each of the three major credit bureaus: The three reporting companies have set up a central website, a toll-free telephone number, and a mailing address through which you can order your free annual report.

To order, visit [annualcreditreport.com](http://annualcreditreport.com). call 1-877-322-8228, or complete the Annual Credit Report Request Form and mail it to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You can print the form from [ftc.gov/credit](http://ftc.gov/credit). Do not contact the three consumer reporting companies individually. They are providing free annual credit reports only through [annualcreditreport.com](http://annualcreditreport.com), 1-877-322-8228, and Annual Credit Report Request Service.

You may order your reports for each of the three consumer reporting agencies at the same time, or you can order your report from each of the companies one at a time. The law allows you to order one free copy of your report every 12 months.

You are also entitled to one free report a year if you're unemployed and plan to look for a job within 60 days, if you're on welfare; or if your report is inaccurate because of fraud, including identity theft, or if you were recently denied credit or a job based on a credit report. When you get your report, look for anything suspicious, such as credit cards and loans or leases that have been wrongfully taken out in your name.

Source: Federal Deposit Insurance Corporation (FDIC), 2008