



**FINANCIAL SERVICES
FOR THE GREATER GOOD®**

Protect Your Financial Identity

Identity theft affects millions of Americans each year. You should take measures to protect yourself.

It can be as simple as someone swiping your purse or as complicated as someone hacking into your credit files. In any case, identity theft — stealing personal data like credit card account information or a Social Security number to make purchases in the victim’s name — has become the most prevalent crime in the United States.

Annually, millions of people are victims of identity theft. Becoming a victim can run into the tens of thousands of dollars, and even higher. Not only can identity thieves steal from you, they can also ruin your name by opening fraudulent accounts that leave you with bad credit, or even a criminal record.

There are simple things you can do to keep your personal information safe from identity thieves.

Online Tips

- Do not reply to an email or pop-up message asking for personal or financial information. Legitimate companies like TIAA-CREF will never ask for personal or financial information via an email or pop-up message.
- Only send personal information to Web pages that are securely encrypted. Look for a closed lock or solid key icon on the page, as well as a URL that begins with “https”; the “s” in the URL indicates that the site is secure.
- Do not write down your passwords, and do not use dates of birth or names of family members as passwords.
- Do not email personal or financial information. If you initiate a transaction, look for indicators that the message is secured, which can be validated by a lock icon at the bottom right-hand (or left-hand) side of most Internet browsers. Most email programs do not provide confidentiality via encryption, so be careful.
- Create “favorites” to access known sites to avoid being lured to imposter sites.
- Be sure to use updated anti-virus software. Some phishing emails contain viruses and software that can harm your computer. (See more on phishing below.)

General Tips

- Shred unwanted documents that contain personal information before putting them in the trash. These include pre-approved credit card applications that you do not want.

- Instruct your credit card company not to send you any blank checks in the mail. If you do receive checks, but do not use them, destroy them thoroughly.
- Review your credit card and bank statements immediately for unauthorized charges and contact the company if statements are more than a few days late.
- Make sure you always take your ATM and credit card receipts after all transactions. You can always shred them later. (If a vendor still uses a “carbon” slip when processing your credit card, ask for it and destroy it.)
- Always report lost or stolen credit and debit cards immediately.

Other Things You Can Do

Check Your Credit Reports Annually. According to the Federal Trade Commission (FTC), the average identity theft victim doesn’t learn he or she has been victimized until a year after the incident occurs. Any of the following events may indicate you’ve been struck by an identity thief: unexplained charges in, or withdrawals from, your accounts; receiving credit cards for which you didn’t apply; not receiving bills or other mail (which may indicate that an identity thief has changed your address); and receiving calls from debt collectors or companies from which you didn’t order products.

The Fair and Accurate Credit Transactions Act of 2003 allows you to get a free credit report from each of the three credit bureaus every 12 months. To better secure your financial credit, you should obtain and review a copy of your report at least once a year. You can get a copy of your report from:

- **Equifax** **800 685-1111**
- **Experian** **888 397-3742**
- **TransUnion** **877 322-8228**

For more information, and to order your free credit report, visit the Federal Trade Commission at **ftc.gov**.

Protect Your Social Security Number. Memorize your Social Security number. Your Social Security number is a thief’s primary tool for opening accounts in your name. Don’t carry your Social Security card or leave it (or the number itself) in an easily accessible place. When making transactions, provide your Social Security number only if absolutely necessary. Find out if you can use other forms of identification, and ask why the organization needs the number, how they will use it and how they plan to safeguard it.

Be Careful on the Phone. Identity thieves often pose as telemarketers, representatives of banks, Internet service providers or even members of government agencies — anything to get you to give out personal information like your Social Security number, date of birth or a mother’s maiden name. So don’t give personal information over the phone or through the mail or Internet unless you’ve initiated the contact or are sure the company is legitimate. If you have any doubts, contact the organization’s customer service department and ask how the information will be used, how it will be secured and who will have access to it.

Nail Down Your Mail. It’s a federal crime to steal mail, but that doesn’t deter identity thieves. Through stolen mail, thieves access credit card applications, bank account statements and other

documents that contain vital personal information. Protect yourself by removing mail from your mailbox promptly. When traveling, contact your post office to receive a “vacation hold” card. When mailing letters or packages, go to the local post office or use post office collection boxes; avoid unsecured mailboxes.

Keep a Lid on Your Trash. Some thieves stoop (literally) to picking through trash or recycling bins to unearth Social Security numbers, account numbers or other personal information. Keep your identity safe by using a crosscut shredder when destroying credit card receipts, statements from financial companies, insurance forms, doctors’ bills and other sensitive personal documents. When you use ATMs, never leave your receipts behind.

Don’t Get “Skimmed.” Identity thieves sometimes obtain ATM pin numbers and other bank account information through a process called “skimming.” A thief attaches a device to an ATM that captures your account information, which is then used to create fake ATM cards in your name. The fake cards are used at other ATMs to access your accounts. Thieves “skim” by placing devices over ATM card readers, or even by inserting tiny cameras in or near the keypad. Avoid ATMs that have unusual features, such as devices attached to the card readers, or a sign telling you to swipe your card through a different reader than the one attached to the screen. Nonbank-related stand-alone ATMs — such as those in convenience stores — are especially susceptible to skimming.

Keep Your Computer Safe. Thieves can hack into computers to access personal information. To safeguard your computer, update your virus protection software regularly. Also, install a firewall to prevent hackers from accessing your system. Don’t download software from sites you aren’t familiar with. If you make online financial transactions, be wary of “phishing,” a scam through which thieves send e-mails or pop-up messages that request information like Social Security numbers and credit card account numbers. Generally, the wording in phishing communications is often careless and contains misspellings. If you receive an email claiming to be from TIAA-CREF that seems fraudulent, please forward it to us immediately at abuse@tiaa-cref.org.

Also be aware of “pharming,” one of the newest scams, in which thieves hijack a domain name system (DNS) and then redirect the URL to a bogus site. If you receive any suspicious e-mail, delete it immediately. Don’t attempt to respond to it or to click on any enclosed link. For additional information on phishing and identity theft, visit the Federal Trade Commission at ftc.gov and look for the following brochures: “How Not to Get Hooked by 'Phishing' Scam” and “ID Theft: When Bad Things Happen to Your Good Name.”

Lock Down Your Laptop. If you use a laptop, avoid storing important personal or financial information on it. Otherwise, use a “strong” password — a combination of upper- and lowercase letters, numbers and symbols.

Bullying or Frightening Tone. Be suspicious of demanding computer messages that threaten to terminate or suspend your account if you do not quickly respond. They may say that if you fail to update, verify or confirm your personal or account information, access to your accounts will be suspended. Legitimate businesses do not request personal information from you over an unsecured website.

Spoofing. Web spoofing involves a fake website that mimics the legitimate site you were trying to visit. You might land there by accidentally keying in an incorrect web address, or by linking to it from a phishing email.

To make spoof sites appear legitimate, criminals may use the logos, graphics, names and codes of the real company's site. They may also attempt to fake the web address in your browser window and the padlock that appears on your Web screen, all to entice you to believe that it is safe to enter your personal information. If you take the bait, the spoof site may route your information — such as your Social Security number or other personal identification numbers, credit card information or financial account numbers — to criminals.

What to Do If You Become a Victim

If you think you've become an identity theft victim, the FTC recommends following these steps:

Contact the Social Security Administration. Call the Fraud Hotline, **800 269-0271**.

Contact the U.S. Department of Justice. You can visit **www.usdoj.gov/criminal/fraud/idtheft.html** for a list of articles.

File a Complaint with the FTC. The FTC provides assistance to victims of identity theft, as well as a free credit report. You can file your case with the FTC Consumer Response Center, at **ftc.gov**. To learn more, contact the FTC at **877 IDTHEFT (438-4338)**. The FTC Identity Theft Clearing House hotline is **877 438-4338**. Two other helpful FTC websites are **<http://www.consumer.gov/idtheft/>** and **www.consumer.gov/idtheft**, where you can access an online booklet called “*ID Theft: What It’s All About.*”

File a Police Report. Send a copy of the report to creditors to show proof of the crime. Keep a copy of the report.

Create A Fraud Alert Flag. Contact the fraud departments of any of the three major credit bureaus to place a fraud alert on your credit file. These include Equifax (**800 685-1111** or **www.equifax.com**); Experian (**888 397-3742** or **www.experian.com**); and Trans Union (**877 322-8228** or **www.transunion.com**). This alert requests creditors to contact you before making changes to your existing accounts or opening new ones. You can also get a credit report from these three agencies.

Close Affected Accounts. If you know that accounts have been fraudulently opened in your name, close them. If you open new accounts, use new pin numbers and passwords.

© 2007 Teachers Insurance and Annuity Association-College Retirement Equities Fund (TIAA-CREF), New York, N.Y. 10017

C39205