**Identity Theft**

**Protecting Your Financial Identity**

Identity theft is one of the fastest-growing types of financial fraud. Without stealing your wallet, a crook can steal your financial identity with as little information as your social security number. It is also called "account-takeover fraud" or "true-name fraud," and it involves crooks' assuming your identity by applying for credit, running up huge bills and stiffing creditors - all in your name.

**Take these steps to protect yourself:**

1. Get a copy of your credit report from each of the three major credit bureaus (TransUnion, Equifax, Experian) every year. It lists all of the lines of credit in your name. Check to be sure that everything is accurate, that all of the accounts are yours and that accounts you have requested to be closed are marked closed.
2. Keep an eye on your accounts throughout the year by reading your monthly/periodic statements thoroughly. That's an easy way for you to be sure that all of the activity in your accounts was initiated by you.
3. Tear up or shred pre-approved credit offers, receipts and other personal information that link your name to account numbers. Don't leave your ATM or debit/credit card receipt in public trash cans. Crooks (a.k.a dumpster divers) are known to go through trash to get account numbers and other items that will give them just enough information to get credit in your name.
4. If your credit card or other bills are more than two weeks late, you should do three things: First, contact the Postal Service to see if someone has forwarded your mail to another address. Second, contact your bank to ask if the statement or card has been mailed. Third, contact the businesses that send you bills.
5. When you pay bills, don't put them in your mailbox with the red flag up. That's a flashing neon light telling crooks to grab your information. Use a locked mailbox or the post office.
6. Protect your account information. Don't write your personal identification number (PIN) on your ATM or debit card. Don't write your social security number or credit card account number on a check. Cover your hand when you are entering your PIN number at an ATM.
7. Don't carry your Social Security card, passport or birth certificate unless you need it that day. Take all but one or two credit cards out of your wallet, and keep a list at home of your account information and customer service telephone numbers. That way, if your wallet is lost or stolen, you'll only have to notify a few of your creditors and the information will be handy.
8. Never provide personal or credit card information over the phone, unless you initiated the call. Crooks are known to call with news that you've won a prize and all they need is your credit card number for verification. Don't fall for it. Remember the old saying, "if it sounds too good to be true, it probably is."

**Take action if you are a victim:**

1. Financial fraud is a crime; call your local police department.
2. Contact the fraud units of all three credit bureaus. Ask them to "flag" your account, which tells creditors that you are a victim of identity fraud. Also, add a victim's statement to each of your credit bureau reports that asks creditors to contact you in person to verify all applications made in your name.   
     
   **Call the fraud units of the credit bureaus at:**  
     
   - TransUnion Fraud Assistance Department: 800-680-7289  
   - Equifax Fraud Assistance Department: 800-525-6285  
   - Experian Fraud Assistance Department: 888-397-3742
3. Call the Federal Trade Commission's ID Theft hotline at 1 (877) IDTHEFT. The hotline is staffed by counselors trained to help ID theft victims.  For more information on reporting identity theft visit the [Federal Trade Commission](http://www.consumer.ftc.gov/).
4. Notify your banks. They can help you obtain new account numbers for all of your checking, savings and other accounts. Be sure to pick a new PIN number for your ATM and debit cards. Close all of your credit card accounts and open with new account numbers.
5. Notify the Postal Inspector if you suspect mail theft - a felony.
6. Depending on your situation, you may want to contact the Social Security Administration to get a new Social Security number. You also may want to contact your telephone, long distance, water, gas and electrical companies to alert them that someone may try to open an account in your name.
7. Finally, make sure to maintain a log of all the contacts you make with authorities regarding the matter. Write down each person's name, title, and phone number in case you need to re-contact them or refer to them in future correspondence.

**Identity Theft: Don't Be an Easy Target**

With sufficient information, a con artist can become "you" and use your identity to order new credit cards, make counterfeit cards or checks, or otherwise go on a spending spree in your name. It's called identity theft or ID theft, and it's a serious problem.

In general, consumers are protected against liability for unauthorized accounts or transactions. However, innocent victims of ID theft sometimes do suffer losses. And if the crime is not detected early, people may face months or years cleaning up the damage to their reputation and credit rating. The evolution of ID theft includes the spread of fraudulent "phishing" (pronounced "fishing") emails. These are unsolicited emails purportedly from a legitimate source, like your bank, attempting to trick you into divulging personal information.

**Here is our "to do" list for keeping your identity to yourself.**

1. Protect your Social Security number (SSN), credit card and debit card numbers, PINs (personal identification numbers), passwords and other personal information.
2. Never provide your personal information in response to an unsolicited request - whether it is over the phone or over the Internet.
3. Protect your incoming and outgoing mail.
4. Keep a close watch on your bank account statements and credit card bills.
5. Exercise your rights to review your credit report and report fraudulent activity - ask us about the new Fair and Accurate Credit Transactions Act (FACTA)
6. Keep your financial trash "clean" - shred your personal financial information

Your personal and financial information can be as good as cash to a criminal. So, take ID theft seriously.

**Manage Your Mailbox**

* Do not leave bill payment envelopes clipped to your mailbox or inside with the flag up; criminals may steal your mail and change your address.
* Know your billing cycles, and watch for any missing mail. Follow up with creditors if bills or new cards do not arrive on time. An identity thief may have filed a change of address request in your name with the creditor or the post office.
* Carefully review your monthly accounts, credit card statements and utility bills (including cellular telephone bills) for unauthorized charges as soon as you receive them. If you suspect unauthorized use, contact the provider's customer service and fraud departments immediately.
* When you order new checks, ask when you can expect delivery. If your mailbox is not secure, then ask to pick up the checks instead of having them delivered to your home.
* Although many consumers appreciate the convenience and customer service of general direct mail, some prefer not to receive offers of pre-approved financing or credit. To "opt out" of receiving such offers, call (888) 5 OPT OUT sponsored by the credit bureaus.
* The Direct Marketing Association offers services to help reduce the number of mail and telephone solicitations. To join their mail preference service, mail your name, home address and signature to: Mail Preference Service, Direct Marketing Association, P. O. Box 9008, Farmingdale, NY 11735-9008.

**Check Your Purse or Wallet**

* Never leave your purse or wallet unattended - even for a minute.
* Protect your PINs (don't carry them in your wallet!) and passwords.
* Carry only personal identification and credit cards you actually need in your purse or wallet. If your I.D. or credit cards are lost or stolen, notify the creditors immediately, and ask the credit bureaus to place a "fraud alert" in your file.
* Keep a list of all your credit cards and bank accounts along with their account numbers, expiration dates and credit limits, as well as the telephone numbers of customer service and fraud departments. Store this list in a safe place.
* If your state uses your Social Security number as your driver's license number, ask to substitute another number.

**Keep Your Personal Numbers Safe and Secure**

* When creating passwords and PINs (personal identification numbers) do not use any part of your Social Security number, birth date, middle name, wife's name, child's name, pet's name, mother's maiden name, address, consecutive numbers, or anything that a thief could easily deduce or discover.
* Ask businesses to substitute a secret alpha-numeric code as a password instead of your mother's maiden name.
* Shield the keypad when using ATMs or when placing calling card calls.
* Memorize your passwords and PINs; never keep them in your wallet, purse, Rolodex or electronic organizer.
* Get your Social Security number out of circulation and release it only when necessary -- for example, on tax forms and employment records, or for banking, stock and property transactions.
* Do not have your Social Security number printed on your checks, and do not allow merchants to write your Social Security number on your checks. If a business requests your Social Security number, ask to use an alternate number.
* Never give your Social Security number, account numbers or personal credit information to anyone who calls you.

**Bank, Shop, and Spend Wisely**

* Store personal information in a safe place and shred or tear up documents you don't need. Destroy charge receipts, copies of credit applications, insurance forms, bank checks and statements, expired charge cards and credit offers you get in the mail before you put them out in the trash.
* Cancel your unused credit cards so that their account numbers will not appear on your credit report.
* When you fill out a loan or credit application, be sure that the business either shreds these applications or stores them in locked files.
* Tear up receipts, bank statements and unused pre-approved credit card offers and convenience checks before throwing them away.
* When possible, watch your credit card as the merchant completes the transaction.
* Use credit cards that have your photo and signature on the front.
* Sign your credit cards immediately upon receipt.
* Carefully consider what information you want placed in the residence telephone book and ask yourself what it reveals about you.
* Keep track of credit card, debit card and ATM receipts. Never throw them in a public trash container. Tear them up or shred them at home when you no longer need them.
* Ask businesses what their privacy policies are and how they will use your information: Can you choose to keep it confidential? Do they restrict access to data?
* Choose to do business with companies you know are reputable, particularly online.
* When conducting business online, use a secure browser that encrypts or scrambles purchase information and make sure your browser's padlock or key icon is active.
* Don't open e-mail from unknown sources. Use virus detection software.

**Review Your Information**

* Order a copy of your credit report from the three credit reporting agencies every year and make sure all the information is correct, especially your name, address, and Social Security number. Look for indications of fraud, such as unauthorized applications, unfamiliar credit accounts, credit inquiries and defaults and delinquencies that you did not cause.
* Check your Social Security Earnings and Benefits statement once each year to make sure that no one else is using your Social Security number for employment.