Protect Yourself From Identity Theft

Identity theft occurs when a criminal uses another person's personal information to take on that person's identity. Identity theft is much more than misuse of a Social Security number, it can also include credit card and mail fraud. If you think you may be a victim of identity theft, contact the Federal Trade Commission (FTC) to report what happened. You can call the FTC's ID Theft Hotline at **1-877-IDTHEFT** (438-4338) for up-to-date information about how to work with credit bureaus and law enforcement agencies to reclaim your identity. Identity theft is the fastest growing financial crime in America with approximately 750,000 cases annually.

How do thieves get your information?

- They go through your trashcan looking for straight cut or un-shredded papers. This is known as dumpster diving.
- They steal your mail or your wallet.
- They listen in on conversations you have in public.
- They trick you into giving them the information over the telephone or by email.
- They buy the information either on the Internet or from someone who might have stolen it.
- They steal it from a loan or credit application form you filled out or from files at a hospital, bank, school or business that you deal with. They may have obtained it from dumpsters outside of such companies.
- They get it from your computer, especially those without firewalls.
- They may be a friend or relative or someone who works for you who has access to your information.

What can you do to protect yourself?

- Do not reveal personal information until you know how it will be used and if it will be shared with others.
- Pay attention to your credit card billing cycles. If a bill is missed it could mean that your account has been taken over by an identity thief and the billing address changed.
- Do not carry other documents in your wallet that have your SS# on them except on days you need them.
- Consider purchasing identity theft insurance, which provides reimbursement to victims of crime for the cost of restoring their identity and repairing credit reports.

    - Some insurance companies offer this coverage as an “add on” to homeowners or renters insurance for a minimal fee of approximately $25.00. The coverage may differ from one company to another in amount of coverage, the deductible and coverage limitations.
    - Some insurance companies offer “stand alone” policies for $60 - $180 per year.
    - Some credit card companies offer insurance coverage for identity theft
- Sign up for the Federal Trade Commission's National Do Not Call Registry and the Direct Marketing Association's Telephone Preference Service. National Do Not Call Registry, www.donotcall.gov, 1-(888) 382-1222. Your name is added to name deletion lists used by nationwide marketers. Register with Louisiana's "do not call" list through the Louisiana Public Service Commission at http://www.lpsc.org/dncprogram.asp
- Have your name and address removed from the phone book and reverse directories.
- Opt-out of the sale or sharing of your financial information when given the opportunity by your bank, credit card companies, insurance companies, and investment firms.
- Install a locked mailbox at your residence to deter mail theft. Use a post office box or a commercial mailbox service. When you are away from home for an extended time, have your mail held at the Post Office, or ask a trusted neighbor to pick it up.
- When ordering new checks, pick them up at the bank. Don't have them mailed to your home. If you have a post office box, use that address on your checks rather than your home address so thieves will not know where you live.
- When you pay bills, do not leave the envelopes containing your checks at your mailbox for the postal carrier to pick up, or in open boxes at the receptionist's desk in your workplace. If stolen, your checks can be altered and then cashed by the imposter. It is best to mail bills and other sensitive items at the drop boxes *inside* the post office rather than neighborhood drop boxes.
- Do not carry extra credit cards, social security card, or birth certificate in your wallet. Store them in a safe place.
- Reduce the number of credit cards you actively use to a minimum. Carry only one or two of them in your wallet. Consider canceling unused accounts. Even though you do not use them, their account numbers are recorded in your credit report, providing a tempting target for identity thieves. But, be aware that reducing the number of credit card accounts *might* lower your credit score. Having credit cards and installment loans and making timely payments determine part of your score.

- Keep a list or photocopy of all your credit cards, bank accounts, and investments -- the account numbers, expiration dates and telephone numbers of the customer service and fraud departments -- in a secure place (not your wallet or purse), so you can quickly contact these companies in case your credit cards have been stolen or accounts are being used fraudulently.
- Never give out your SSN, credit card number or other personal information over the phone, by mail, or on the Internet unless you have a trusted business relationship with the company and *you* have initiated the call. Identity thieves have been known to call their victims with a fake story that goes something like this. "Today is your lucky day! You have been chosen by the Publishers Consolidated Sweepstakes to receive a free trip to the Bahamas. All we need is your Social Security number, credit card number and expiration date to verify you as the lucky winner."
- Always take credit card receipts with you. Never toss them in a public trash container. When shopping, put receipts in your wallet rather than in the shopping bag.
- Never permit your credit card number to be written onto your checks because it puts you at risk for fraud.
- Watch the mail when you expect a new or reissued credit card to arrive. Contact the issuer if the card does not arrive.
- Order your credit report once a year, or better twice, from each of the three credit bureaus to check for errors and fraudulent use of your accounts. Credit reports cost $8-$9 in most states. If you are on a budget, order from one credit bureau now, from another in six months, and the third six months later. In one year you will have checked all three. Beginning in December 2004, consumers can get a free copy of their credit report annually. Free annual credit reports will be rolled out starting on the West Coast December 1, 2004, and ending in September 2005 on the East Coast. To order your free reports when they become available in your state, go to www.annualcreditreport.com where you can order your reports directly or download the Annual Credit Report Request form to mail in your request. You can also call 877-322-8228. For more information, see the Federal Trade Commission's Facts for Consumers at www.ftc.gov/bcp/conline/pubs/credit/freereports.htm.
- Have your name removed from the marketing lists of the three credit bureaus - Equifax, Experian (formerly TRW) and Trans Union. **Call 888-5OPTOUT**. This will limit the number of pre-approved offers of credit that you receive.
- You do not have to be an identity theft victim to place a "fraud alert" on your three credit reports. With the alerts, you place a statement on your files requesting credit issuers to call you at your phone number before issuing credit.

In theory, anyway, if an imposter attempts to open credit in your name, the credit grantor will contact you first. But they do not always pay attention to fraud alerts, so this strategy does not ensure that you'll prevent identity theft. When you place fraud alerts by phone, the credit bureaus give you a temporary alert, good for only a few months. If you wish to extend the fraud alert, you must write the three credit bureaus and request a *seven-year* fraud alert. For information on how to establish fraud alerts, read "step one" of the PRC's Fact Sheet 17a, www.privacyrights.org/fs/fs17a.htm.

- When creating passwords and PINs (personal identification numbers), do not use the last four digits of your Social Security number, mother's maiden name, your birth date, middle name, pet's name, consecutive numbers or anything else that could easily be discovered by thieves. It's best to create passwords that combine letters and numbers.
- Ask your financial institutions to add extra security protection to your account. Most will allow you to use an additional code or password (a number or word) when accessing your account. Do not use your mother's maiden name, SSN, or date of birth. Identity thieves easily obtain this information.
- Memorize all your passwords. Don't record them on anything in your wallet.
- Shield your hand when using a bank ATM machine or making long distance phone calls with your phone card. "Shoulder surfers" may be nearby with binoculars or video cameras.
- Protect your Social Security number (SSN). Release it only when absolutely necessary (like tax forms, employment records, most banking, stock and property transactions). The SSN is the key to your credit and banking accounts and is the prime target of criminals. If a business requests your SSN, ask if it has an alternative number that can be used instead. Speak to a manager or supervisor if your request is not honored. Ask to see the company's written policy on SSNs. If necessary, take your business elsewhere. If the SSN is requested by a government agency, look for the Privacy Act notice. This will tell you if your SSN is required, what will be done with it, and what happens if you refuse to provide it. If your state uses your SSN as your driver's license number, ask to substitute another number.
- Do not have your SSN or driver's license number printed on your checks. Don't let merchants hand-write the SSN onto your checks because of the risk of fraud. There is no law against this, so you may need to be assertive.
- Examine your Social Security Personal Earnings and Benefits Estimate Statement each year to check for fraud. The Social Security Administration mails it to adult-age SSN holders about three months before their birthday. The

SSA web site has additional information, www.ssa.gov/mystatement. Reach them by phone at (800) 772-1213.

- Do not carry your SSN card in your wallet except for situations when it is required, the first day on the job, for example. If possible, do not carry wallet cards that display the SSN, such as insurance cards, except when needed to receive healthcare services.
- If you live in a state that uses the SSN as the driver's license number, we recommend that you contact your Department of Motor Vehicles and request a different number.
- Install a firewall on your home computer to prevent hackers from obtaining personal identifying and financial data from your hard drive. This is especially important if you connect to the Internet by DSL or cable modem.
- Delete without replying to any suspicious email requests.
- Install and update virus protection software to prevent a worm or virus from causing your computer to send out files or other stored information.
- Password-protect files that contain sensitive personal data, such as financial account information. Create passwords that combine 6-8 numbers and letters, upper and lower case.
- When shopping online, do business with companies that provide transaction security protection, and that have strong privacy and security policies.
- Before disposing of your computer, remove data by using a strong "wipe" utility program. Do not rely on the "delete" function to remove files containing sensitive information.
- Each month, carefully review your credit card, bank and phone statements, including cellular phone bills, for unauthorized use.
- Do not toss pre-approved credit offers in your trash or recycling bin without first tearing them into small pieces or shredding them. They can be used by "dumpster divers" to order credit cards in your name and mail them to their address. Do the same with other sensitive information like credit card receipts, phone bills, bank account statements, investment account reports, and so on. Home shredders can be purchased in many office supply stores. We recommend cross-cut shredders.
- When you fill out loan or credit applications, find out how the company disposes of them. If you are not convinced that they store them in locked files and/or shred them, take your business elsewhere. Some auto dealerships, department stores, car rental agencies, and video stores have been known to be careless with customer applications. When you pay by credit card, ask the business how it stores and disposes of the forms. Avoid paying by credit card if

you think the business is not careful. When paying with credit cards on the Internet, be sure the company uses secure transmission and storage methods.

- Store canceled checks in a safe place. In the wrong hands, they could reveal a lot of information about you, including the account number, your phone number and driver's license number.
- Store personal information securely in your home, especially if you have roommates, employ outside help, or have service work done in your home.

Sources:

Social Security Administration
http://www.ssa.gov/pubs/idtheft.htm

Federal Trade Commission
https://rn.ftc.gov/pls/dod/widtpubl$.startup?Z_ORG_CODE=PU03

Privacy Rights Clearing House
http://www.privacyrights.org/fs/fs2-wire.htm

Identity Theft Resource Center
http://www.idtheftcenter.org/preventiontips.shtml

Louisiana Public Service Commission – Do Not Call List
http://www.lpsc.org/dncprogram.asp