

Protecting Yourself from Identity Theft

What is Identity Theft?

Identity theft is the fraudulent use of a person's personal identifying information. Often, identity thieves will use another person's personal information, such as a social security number, mother's maiden name, date of birth, or account number to open fraudulent new credit card accounts, charge existing credit card accounts, write checks, open bank accounts, or obtain new loans. They may obtain this information by:

- Stealing wallets that contain personal identification information and credit cards
- Stealing bank statements from the mail
- Diverting mail from its intended recipients by submitting a change of address form
- Rummaging through trash for personal data
- Stealing personal identification information from workplace records
- Intercepting or otherwise obtaining information transmitted electronically
- Posing as a legitimate business representative via e-mail or phone to trick people into giving out their information (see below for more information)

Gone Phishing

Phishing, also called "carding" or "web-spoofing" is a high-tech scam that uses spam (unsolicited e-mail that goes out to thousands of e-mail addresses) to deceive people into giving out their credit card numbers, bank account information, Social Security numbers, passwords and other sensitive information. The e-mail messages look like they come from businesses that the potential victims deal with for example, their Internet service provider (ISP), bill pay service or bank. The fraudsters tell recipients that they need to "update" or "validate" their billing information to keep their accounts active, and direct them to a "look-alike" website of the legitimate business, further tricking people into thinking they are responding to a genuine request. Unknowingly, people submit their financial information - not to the businesses - but the scammers, who use it to order goods and services and obtain credit.

Calling on a Pretext

Pretext calling is another fraudulent means of obtaining a person's personal information. Identity thieves can be skilled liars, and may pose as representatives of banks, Internet service providers (ISPs) or even government agencies to get you to reveal identifying information. Pretext callers may contact financial center employees, posing as clients, to access clients' personal account information. Information obtained from pretext calling may be sold to debt collection services, attorneys, and private investigators to use in court proceedings. For your protection, Tennessee Commerce Bank and the TCB Call Center representatives use special "know your caller" procedures to prevent unauthorized distribution of your personal account information.

How to Avoid Becoming a Victim of Identity Theft

Here are some basic steps recommended by the Federal Trade Commission (FTC) that you can take to avoid becoming a victim of identity theft:

Keep Personal and Financial Information Secure:

- Establish and protect passwords/PINs for your credit card, bank and phone accounts. Avoid using easily available information like your mother's maiden name, your birth date, the last four digits of your social security number (SSN) or your phone number, or a series of consecutive numbers. When you're asked for your mother's maiden name on an application for a new account, try using a password instead.

- Secure personal information in your home, especially if you have roommates, employ outside help, or are having service work done in your home.
- Ask about information security procedures in your workplace. Find out who has access to your personal information and verify that your records are kept in a secure location. Ask about the disposal procedures for those records as well.
- Never give out personal or financial information over the phone, through the mail, by e-mail or over the Internet unless you've initiated the contact. Remember a legitimate company would never ask you for your account number or PIN/security code - they assigned them and therefore already have this information. Before you divulge any personal or financial information, confirm that you're dealing with a legitimate representative of a legitimate organization. Double check by calling customer service using the number on your account statement or in the phone book.
- Guard your mail and trash from theft. Deposit outgoing mail in post office collection boxes or at your local post office instead of an unsecured mailbox. Remove mail from your mailbox promptly. If you're planning to be away from home and can't pick up your mail, call the U.S. Postal Service at 1-800-275-8777 to ask for a vacation hold. To thwart a thief who may pick through your trash or recycling bins, tear or shred your charge receipts, copies of credit applications or offers, insurance forms, physician statements, checks and bank statements and expired charge cards.
- Before revealing any identifying information (for example, on an application), ask how it will be used and secured, and whether it will be shared with others. Find out if you have a say in the use of your information. For example, can you choose to have it kept confidential?
- Keep your social security card in a secure place and give your SSN out only when absolutely necessary. Very likely, your employer and financial institution will need your SSN for wage and tax reporting purposes. Other private businesses may ask you for your SSN to do a credit check, such as when you apply for a car loan. Sometimes, however, they simply want your SSN for general record keeping. If someone asks for your SSN, ask the following questions: Why do you need it? How will it be used? How do you protect it from being stolen? Can you use another number such as my driver's license number instead? What will happen if I don't give it to you? Getting satisfactory answers to your questions will help you to decide whether you want to share your SSN with the business.
- Limit the identification information and the number of credit and debit cards that you carry to what you'll actually need. Do not carry your social security card with you.
- Keep your purse or wallet in a safe place at work.

Protect Your Computer Data:

- Always access TCB's website by going to www.tncommercebank.com directly and not through links from other sites or sent in an e-mail message.
- If you get an e-mail that warns you, with little or no notice, that an account of yours will be closed unless you confirm you're billing information, do not reply or click on the link in the e-mail message. Instead, contact the company cited in the message using a telephone number you know to be genuine. TCB does not contact clients via e-mail, phone or mail to request or verify security information about passwords or PINs. Report suspicious activity to the FTC and send the actual e-mail message to uce@ftc.gov.
- Clear your temporary Internet files or cache after you log out of your TCB online banking account especially if you accessed it from a public computer (where others will use the computer after you).
- Update your virus protection software on your computer regularly. Computer viruses can have damaging effects, including introducing program code that causes your computer to send out files or other stored information. Look for security repairs and patches you can download from your operating system's Web site.

- Don't download files from strangers or click on hyperlinks from people you don't know. Opening a file could expose your system to a computer virus or a program that could hijack your modem.
- Use a firewall, especially if you have a high-speed or "always on" connection to the Internet. The firewall allows you to limit uninvited access to your computer. Without a firewall, hackers can take over your computer and access sensitive information.
- Use a secure browser - software that encrypts or scrambles information you send over the Internet - to guard the safety of your online transactions. When you're submitting information, look for the "lock" or "key" icon on the status bar. It's a symbol that your information is secure during transmission. Another sign that a site is secure is the "s" after "http" in the web address "https." The "s" indicates that it is a secure site. To verify the site's security certificate, select "Properties" from your browser's File menu and click on the "Certificates" button or click on the Secure Site Seal.
- Try not to store financial information on your laptop unless absolutely necessary. If you do, use a "strong" password - that is, a combination of letters (upper and lower case), numbers and symbols.
- Avoid using an automatic log-in feature that saves your user name and password; and always log off when you're finished. If your computer gets stolen, the thief will have a hard time accessing sensitive information.
- Delete any personal information stored on your computer before you dispose of it. Use a "wipe" utility program, which overwrites the entire hard drive and makes the files unrecoverable.
- Read web site privacy policies. They should answer questions about the access to and accuracy, security of and control of personal information the site collects, as well as how sensitive information will be used, and whether it will be provided to third parties.

Stay Vigilant:

- Pay attention to your billing cycles. Follow up with creditors if your bills don't arrive on time. A missing credit card bill could mean an identity thief has taken over your account and changed your billing address. Review your statements as soon as you receive them to ensure all charges, checks or withdrawals were authorized.
- Order copies of your credit report from each of the three major credit bureaus at least once a year to ensure that they are accurate.
- Reduce the number of pre-approved and direct mail offers and telephone solicitations by opting out of them.
 - To opt out of pre-approved offers of credit, you can opt out of such offers by calling (888) 5 OPT OUT.
 - To reduce e-mail solicitations, register with the Direct Marketing Association (DMA) E-mail Preference Service at <http://www.dmaconsumers.org/offemalilist.html>.
 - To reduce direct mail solicitations, register with the DMA Mail Preferences Service at <http://www.dmaconsumers.org/offmailinglist.html>.
 - To reduce telemarketing solicitations, register with the DMA Telephone Preference Service at <http://www.dmaconsumers.org/offtelephonest.html>. You can also register with a state "do not call list" and the FTC National Do Not Call List by going to <http://www.ftc.gov/donotcall/> or by calling 1-888-382-1222 from the number you wish to register. Note: The FTC does not allow third-parties to "pre-register" people for the registry. Websites or phone solicitors that claim they can or will register your name or phone number on a national list - especially those who charge a fee - are a scam.
- If you don't want to receive telemarketing calls from particular sellers, you can limit them by telling the company to put your number on its company do not call list. The company-specific do not call

rules apply to all telemarketing calls, including calls from companies with which you have done business and telemarketing calls on behalf of charities.

If You Become a Victim of Identity Theft

If you think that someone has stolen your identity, you should:

- Report the incident to TCB's Bank Security by calling 1-877-684-2265.
- Contact Tennessee Commerce Bank and any other financial institutions where you have an account that you think may be the subject of identity theft. Advise them of the identity theft. Request that they restrict access to your account, change your account password, or close your account, if there is evidence that your account has been the target of criminal activity. If you close your account, ask them to issue you a new credit card, ATM card, check card, or checks, as appropriate.
- Contact the fraud department of each of the major credit bureaus to report it and request that they place a fraud alert and a victim's statement in your file. The fraud alert puts creditors on notice that you have been the victim of fraud, and the victim's statement asks them not to open additional accounts without first contacting you. These are the phone numbers for the fraud departments of the three national credit bureaus:
Trans Union: 1-800-916-8800;
Equifax: 1-800-685-1111;
Experian: 1-888-397-3742
- Request a free copy of your credit report. Credit bureaus must provide a free copy of your report, if you have reason to believe the report is inaccurate because of fraud and you submit a request in writing. Review your report to make sure no additional fraudulent accounts have been opened in your name, or unauthorized changes made to your existing accounts. Also, check the section of your report that lists "inquiries" and request that any inquiries from companies that opened the fraudulent accounts be removed.
- File a report with your local police department.
- File a complaint with the FTC at <http://www.ftc.gov/> or call the FTC Identity Theft Hotline toll-free at 1-877-ID-THEFT. The FTC puts the information into a secure consumer fraud database and shares it with law enforcement agencies.