Identity Theft and Financial Crimes

Anyone can fall victim to identity theft, regardless of your age, race, or socioeconomic status. If you suspect you or someone you know may have been a victim of identity theft, it is important to take action now to stop further use of your identity.

Identity Theft Victim Tips:

One of the first things that a victim should do is report the incident to the Shelby County Sheriff's Office or to their local law enforcement agency.

The Federal Trade Commission (FTC) https://www.ftc.gov/ has developed an online one-stop resource that provides an interactive, step-by-step guide in reporting and steps to follow to assist in the recovery process. The FTC maintains the latest information on current scams and offers tips and advice to avoid becoming a victim.

IdentityTheft.gov https://www.identitytheft.gov/ allows victims to file complaints, receive personal recovery plans, and to educate consumers on a variety of financial issues, new frauds and scams, and other resources. This interactive investigative tool may also refer victim complainants to other appropriate agencies for further action. IdentityTheft.gov allows victims to enter and track their progress on a secure site that walks them through each step of the process by providing follow-up reminders; instructing the user to notify other grantors, institutions, and businesses to report the fraudulent use; generating customized letters, affidavits, and forms to send to their creditors, debt collectors, credit reporting agencies, and to the Internal Revenue Service.

How to Prevent Becoming a Victim:

- Report lost or stolen credit cards immediately.
- If you applied for a credit card or are expecting a replacement card and did not receive it when expected, call the issuing financial institution.
- Sign new credit cards immediately, before someone else does.
- Memorize your Social Security number and all passwords. Do not use your date of birth or some other important date as your password, and do not record passwords on papers that you carry with you. If you need to record passwords, leave them in a secure location.
- Beware of telephone solicitations asking for personal information about your accounts or your social security number. Never give personal information over the telephone, such as your social security number, date of birth, mother's maiden name, credit card number or bank PIN number, unless you initiated the call. Make sure you release this information only when necessary.

- Do not give out your social security number freely.
- Never leave transaction receipts at an ATM, a store counter, gasoline pumps or trash cans.
- Save all credit card receipts and match them against your monthly bill. Check your monthly financial statements for accuracy. If you do not receive your statements when expected, contact the sender.
- Keep track of all paperwork and destroy what you no longer need. Shred all bills, credit card charge receipts, credit applications, insurance forms, bank statements, expired charge cards, and pre-approved credit offers before throwing them into the garbage.
- Do not carry your Social Security card or birth certificate with you, but leave those in a secure location.
- Do not disclose credit card or other financial account number over the phone or on a Website unless the site offers a secure transaction indicated by:
    - An icon of a lock will appear in the bottom strip of the Web browser page.
    - The URL for the Webpage will change from "http" to "https" for the page at which you input the personal date. The "https" indicates the URL is a secure site.
- Beware of mail or telephone solicitations that offer prizes or awards, especially if the person making the offer asks you for personal information or financial account information. If you are going out of town or will be away from your home for an extended period of time, contact the United States Postal Service to place a hold on your curbside mail to help prevent your mail from being stolen from your mailbox, which may contain financial documents. You can access this service by calling 1-800-275-8777, or online at https://holdmail.usps.com/holdmail/.
- Place outgoing mail in post office collection boxes or at your local post office.
- Do not provide personal information simply because someone asks for it or because it is asked for on a form, questionnaire or product registration card.
- Do not carry extra credit cards in your wallet or pocketbook. Cancel the ones you no longer use.
- Order free credit bureau credit reports once a year to check for fraudulent activity or other discrepancies.
- Never loan anyone your credit/debit cards.
- Notify all banks and credit card companies of any change of address.
- Never put bank account or credit card numbers on the outside of an envelope or postcard.
- When disclosing credit card, checking account or other financial data online, use caution. Make sure you receive a secured authentication key (lock icon) and a statement that indicates your transaction is secure.
- Be cautious of e-mails and instant messages that are unsolicited and request you to confirm credit card numbers, passwords or other personal information. Con artists often pose as agents of banks, on-line shopping services or internet providers attempting to obtain this information to commit fraud.
- Financial institutions may share your information with other companies. If you want, you can limit some of that sharing. Each year, your financial institutions should send you a privacy notice with instructions for "opting out." Read these notices carefully. Also, when establishing accounts with new companies, ask about privacy policies and make your wishes known.

- The credit bureaus offer a toll-free number that enables you to "opt-out" of having pre-approved credit offers sent to you for two years. Call 1-888-5-0PTOUT, (567-8688) for more information.
- The Federal Government has created the National Do Not Call Registry. To register, or get information, visit www.donotcall.gov, or call 1-888-382-1222 from the phone you want to register. You will receive fewer telemarketing calls once your number has been on the registry for 31 days, there is no renewal process, and you can register your home and mobile numbers.

Credit Reporting Agencies

If you are a victim of identity theft, contact the credit reporting agencies and inform them that you are a victim, and ask them for names and telephone numbers of credit grantors with whom fraudulent accounts have been opened. Ask the credit reporting agencies to remove inquiries that have been generated due to the fraudulent access. Ask them to place a fraud alert on your credit report and request that they contact you personally prior to the opening of any new accounts. The credit reporting agencies and their contact information are:

Equifax
www.equifax.com
1-800-525-6285

Experian
www.experian.com
1-800-397-3742

Transunion
www.transunion.com
1-800-680-7289.

Additional Resources and Information:

United States Postal Inspectors **https://postalinspectors.uspis.gov/**
United States Secret Service **http://www.secretservice.gov/**
Federal Bureau of Investigations **https://www.fbi.gov/about-us/investigate/cyber/identity_theft/identity-theft-overview**
U.S. Department of Justice https://www.justice.gov/criminal-fraud/identity-theft/identity-theft-and-identity-fraud.