

Preventing Identity Theft



Almost every day, the average consumer writes a check, uses a credit card to buy something on line, uses an ATM machine or engages in some other act of information sharing that could open the door to identity theft. To help consumers conduct these routine activities with confidence, Family Foundations has assembled a list of tips to reduce the risk of identity theft.

- **Never give out personal or account information in response to a phone or e-mail query unless it is part of a transaction that you initiated.** Identity thieves are becoming more savvy, often posing as a legitimate bank or financial institution claiming that there is a problem with your account, a technique known as “phishing.” As part of these “phishing” schemes, the identity thief will ask for personal information such as a personal identification number (PIN), Social Security number (SSN) or even account numbers.
- **Open credit card and other bills promptly and reconcile receipts and accounts.** Just because your credit card and/or ATM card is still in your wallet doesn’t mean that you’re not still at risk of identify theft. “Skimming” or stealing credit card or debit card numbers by capturing your information stored with your creditor, retailer, or elsewhere is also a popular means of identify theft.
- **Treat paper and electronic mail carefully.** “Dumpster diving,” or the act of rummaging through trash, is another way identity thieves can obtain personal information. Thieves also can use sophisticated computer techniques to obtain personal information stored on your computer or to access personal information during online transactions. To combat this, you should be sure to:
 - Deposit outgoing mail in secured mailboxes, such as a U.S. Post Office box.
 - Tear or shred charge receipts, copies of credit applications, bills, bank statements and other documents bearing personal information.
 - Be cautious about using a personal computer or laptop to store personal information.
 - Update virus protection software regularly and use both a firewall and secure browser.
- **Check your credit reports with the three major credit bureaus once a year or consider purchasing a service that alerts you to any request for your credit information or unusual activity on your account.** You are entitled to a free copy of your credit report every 12 months. Visit www.annualcreditreport.com to receive a copy of your credit report.

- **Become a cautious guardian of your personal information.** This means following a series of common sense steps to guard your financial privacy, such as signing new credit and debit cards immediately when they arrive. Keep a record of account numbers, expiration dates and the phone number and address of each company in a secure location with limited access. Do not carry your Social Security card with you, but rather keep it in a secure location.

Recovering from Identify Theft

You've followed the tips outlined above but still believe that your personal information has been compromised. What should you do to address the situation and protect your financial well being?

- **Report any suspicious activity or fraudulent charges to your financial institution immediately.** Most of the time the complaint needs to be filed in writing.
- **Place a fraud alert on your credit reports and continue to review your reports periodically.** There are two types of fraud alerts: an initial alert that lasts 90 days and an extended alert that stays on your report for seven years. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you. When reviewing your reports, look for accounts that you did not open or debts that you cannot explain. Follow the regulations set by each of the three credit bureaus to have fraudulent information removed.
- **Close the account(s) that you know or believe has been compromised or fraudulently opened.** If the fraud occurred on a cash account, such as a checking or savings account, be sure to reconcile any outstanding checks, withdrawals or deposits before closing the account.
- **File a complaint with the Federal Trade Commission and your local police.** Be certain to keep track of all reports that the police file on your behalf. You may need these reports to prove that you have been a victim of identify theft where fraudulent charges and/or accounts have occurred.
- **Take the appropriate steps to correct fraudulent information on your credit report.** The Fair Credit Reporting Act (FCRA) establishes a series of procedures for consumers to have their fraudulent information removed from credit reports. The process, however, can be a long and daunting one. Don't feel like you have to complete the process alone. Reach out for assistance. One option is to contact Family Foundations at (904)396-4846 to find a certified credit counselor who can help guide you through the identity theft recovery process.

Family Foundations stands ready to help. To reach us, call (904) 396-4846 or go online to www.familyfoundations.org.

About Family Foundations

You don't have to solve your financial problems alone. Family Foundations has trained and certified credit counselors who offer financial management and debt reduction services. Family Foundations is a nonprofit, community-based organization and a Member of the National Foundations for Credit Counseling (NFCC). For more information on Family Foundations, call (904) 396-4846 or visit www.familyfoundations.org.