

Identity theft is an increasingly serious crime that occurs when an unauthorized person uses or transmits your personal information, such as your name, Social Security number, bank or credit account numbers, or other identifying information, without lawful authority, to commit financial fraud or other crimes.

Identity Theft

Some forms of financial fraud related to identity theft can be more damaging to victims than others. Payment card fraud — unauthorized use of existing payment cards or card numbers — is one type that has been reasonably well managed by the payment cards industry. Card issuers can cancel the compromised card account and issue a new card and account number to the victim to stop further misuse. Also, in most cases, federal law limits victims' liability for the fraudulent use of their payment cards. For more information on payment card fraud and steps consumers can take to safeguard their card account information, the Federal Reserve Bank of Philadelphia has published a complementary brochure titled *Preventing Payment Card Fraud: Dos and Don'ts*.

In its most damaging form, identity theft can mean a person's entire financial identity has been stolen and used to establish new credit without the victim's awareness. The new credit is tied to account information with mailing addresses that are accessible to the identity thief and are no longer tied to the real consumer. Early detection of this type of fraud is difficult because victims do not receive account information — such as statements — that would alert them to the fraud.

Typically, victims become aware of such fraudulently established accounts only after reviewing their credit reports, receiving calls from collection agencies, or being denied credit. Victims can face a time-intensive clean-up process in order to restore their credit records. This generally means that the victim must contact all credit providers on their credit report, dispute fraudulent accounts and transactions, and file police reports. The government and the payment cards industry have made significant progress in providing victims with tools to protect their personal data, to limit consumer liability, and to streamline the clean-up process. Credit report freeze laws, enacted by the states, and the Fair and Accurate Credit Transactions Act (FACT Act), which was passed in December 2003, are major pieces of legislation aimed at helping to combat this form of financial fraud.



To minimize your risk of identity theft, particularly as it relates to the creation of new credit accounts, you can take several steps. First and foremost, it is important to manage your personal information wisely, be aware of the issues, and think about taking care of your identity as something you must do regularly. In addition, taking the following steps will help you to safeguard your personal and financial information.

- 1. Order copies of your credit report from each of the three national credit bureaus every year.** Consumers should review their credit report for unauthorized activity that might be the result of identity theft. In December 2003, President George W. Bush signed into law the Fair and Accurate Credit Transactions Act (FACT Act). This legislation requires, among other things, that the three nationwide credit bureaus — Equifax, Experian, and TransUnion — provide consumers, upon request, a free copy of their credit report once every 12 months. To obtain a free copy of your credit report from one or all three of the national credit bureaus, visit www.annualcreditreport.com or call 1-877-322-8228. To request your report(s) through the mail, visit www.annualcreditreport.com/cra/order?mail, fill out the form, print it, and then mail it to:

Annual Credit Report Request Service
P.O. Box 105281
Atlanta, GA 30348-5281

- 2. Pay attention to your billing cycles and always review your monthly statements for inaccuracies.** 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 payment card account and changed your billing address to cover his tracks. Also, be sure to verify that all transactions have been made with your authorization and to promptly dispute, in writing to your payment card issuer, any fraudulent activity.

Make sure you tear up or shred your credit card receipts, copies of credit applications, insurance forms, physician statements, canceled bank checks, and statements you are discarding.



- 3. Destroy sensitive documents prior to discarding them.** To prevent an identity thief, who may pick through your trash or recycling bins, from stealing your personal information, make sure you tear up or shred your credit card receipts, copies of credit applications, insurance forms, physician statements, canceled bank checks, and statements you are discarding. Also, destroy expired payment cards and any unused credit offers you get in the mail.
- 4. Do not provide personal information on the phone, through the mail, or over the Internet unless you have initiated the contact or you know the party requesting the information.** Identity thieves may pose as representatives of banks, Internet service providers, and even government agencies to get you to reveal your Social Security number, financial account numbers, and other identifying information. These types of scams can be perpetrated in person, over the phone, on the Internet, and through e-mail. Be especially wary of unsolicited e-mails that ask for personal or financial information.
- 5. Keep items with personal information in a secure place.** Be cautious about where you leave personal information in your home, especially if you have roommates, employ outside help, or are having service work done in your home. Do not keep PINs (personal identification numbers) near your checkbook, ATM cards, credit card, or debit card. It is important to keep a record — in a safe place, separate from your cards — of your account numbers, their expiration dates, and the phone number and address of the card-issuing bank for each card so you can quickly report fraudulent activity.
- 6. Guard your mail from theft.** Deposit outgoing mail in post office collection boxes or at your local post office. Promptly remove mail from your mailbox after it has been delivered. If you're planning to be away from home and can't pick up your mail, contact the U.S. Postal Service to request a vacation hold. The Postal Service will hold your mail at your local post office until

you can pick it up. You can also consider putting a lock on your mailbox or using a post office box to receive mail.

7. **Give your Social Security number only when absolutely necessary.** Ask to use other types of identifiers when possible. Do not carry your Social Security card with you; keep it in a safe place.
8. **Find out how personal identifying information will be used and whether it will be shared with others before you reveal it.** Ask if you can choose to have it kept confidential.
9. **Protect your account access with passwords; be sure to use passwords that are difficult to guess.** Putting passwords on your credit card, bank, and phone accounts will ensure that only you can talk with company representatives about your accounts. Do not use easily identifiable information, such as your mother's maiden name, your birth date, the last four digits of your Social Security number, or your phone number, as passwords.
10. **Limit identification information and carry only those cards you will need.** Keep cards separate from your wallet, in a zippered compartment, business card holder, or small pouch.

Even if you have been careful to protect your personal data, an identity thief still may strike. If your wallet or purse has been lost or stolen, you are at risk. In addition, if your monthly statements have not arrived as expected or if you have received calls from either issuers or collection agencies regarding transactions or accounts of which you are unaware, it may mean that someone has stolen your personal information and is using it to commit identity theft–related fraud. If you suspect you might be a victim of identity theft, take the following steps immediately:

1. **Place a fraud alert on your credit file by calling any one of the three national credit bureaus.** This can help prevent an identity thief from opening additional accounts in your name. As

Protect your account access with passwords; be sure to use passwords that are difficult to guess.



soon as the credit bureau confirms your fraud alert, it will automatically notify the other two credit bureaus. The other bureaus will then place fraud alerts on your reports. In addition, once you have notified a credit bureau of suspected fraud, the bureau must make an additional credit report available to you, at your request, free of charge. To place a fraud alert on your credit file, call the toll-free number of one of the three national credit bureaus:

Equifax:	1-888-766-0008
Experian:	1-888-397-3742
TransUnion:	1-800-680-7289

- 2. Review credit reports from each of the three national credit bureaus for inaccuracies and possible fraudulent accounts, inquiries, and transactions.** Once you receive your credit reports, review them carefully to make sure no fraudulent accounts have been opened in your name or unauthorized changes made to your existing accounts. You should continue to check your reports periodically, especially in the first year of discovery, to make sure no new fraudulent activity has occurred.
- 3. Contact the fraud department of your primary lender as well as those at banks, credit card companies, utilities, telephone companies, and Internet service providers with which you do business.** Close accounts that have been tampered with and dispute fraudulent charges on these accounts. After reviewing your credit reports, call the fraud departments of any additional accounts listed on the reports that appear to be fraudulently opened using your personal information. It's particularly important to follow up oral notification in writing to each company.
- 4. File a report with your local police or the police in the community where the identity theft took place.** Creditors will request a copy of this report to provide additional verification that identity theft has occurred.

- 5. File a complaint with the Federal Trade Commission (FTC).** The FTC maintains a database of identity theft cases; law enforcement agencies use it for investigations. Filing a complaint will also help the FTC to learn more about this crime and to better help those who are victimized by identity thieves.

To file a complaint or for more information on identity theft, how to protect your personal information, and what to do if you become a victim, visit the Federal Trade Commission's website: www.ftc.gov/bcp/edu/microsites/idtheft.

To obtain a free copy of your credit report from one or all three of the national credit bureaus, visit www.annualcreditreport.com or call 1-877-322-8228. To request your report(s) through the mail, visit www.annualcreditreport.com/cra/order?mail, fill out the form, print it, and then mail it to:

Annual Credit Report Request Service
P.O. Box 105281
Atlanta, GA 30348-5281



To view this and other consumer publications produced by the Federal Reserve Bank of Philadelphia, scan your smartphone here.



FEDERAL RESERVE BANK
OF PHILADELPHIA

Ten Independence Mall
Philadelphia, PA 19106

www.philadelphiafed.org