

If You Become a Victim of Identity Theft

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

- **Contact the fraud department** of each of the three major credit bureaus to report the identity theft and request that the credit bureaus 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.

The following are the telephone numbers for the fraud departments of the three national credit bureaus:

Trans Union: 1-800-680-7289;

Equifax: 1-800-525-6285;

Experian: 1-888-397-3742.

You may 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.

- **Contact any bank or other creditor 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 your bank closes your account, ask them to issue you a new credit card, ATM card, debit card, or checks, as appropriate.
- **File a report with your local police department.**
- **Contact the FTC's Identity Theft Hotline toll-free at 1-877-ID-THEFT (438-4338).** The FTC puts the information into a secure consumer fraud database and shares it with local, state, and federal law enforcement agencies.



Comptroller of the Currency
Administrator of National Banks

How to Avoid Becoming a Victim of Identity Theft



What is Identity Theft?

Here are a few basic steps you can take to avoid becoming a victim of identity theft and pretext calling:

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.

Pretext calling is a fraudulent means of obtaining a person's personal information.

Pretext callers may contact bank employees, posing as customers, to access customers' personal account information. Information obtained from pretext calling may be sold to debt collection services, attorneys, and private investigators to use in court proceedings. Identity thieves may also engage in pretext calling to obtain personal information to create fraudulent accounts.

- **Do not give personal information**, such as account numbers or social security numbers, over the telephone, through the mail, or over the Internet, unless you initiated the contact or know with whom you are dealing.
- **Store personal information in a safe place** and tear up old credit card receipts, ATM receipts, old account statements, and unused credit card offers before throwing them away.
- **Protect your PINs and other passwords.** Avoid using easily available information, such as your mother's maiden name, your birth date, the last four digits of your social security number, your phone number, etc.
- **Carry only the minimum amount of identifying information** and number of credit cards that you need.
- **Pay attention to billing cycles and statements.** Inquire of the bank, if you do not receive a monthly bill. It may mean that the bill has been diverted by an identity thief.
- **Check account statements carefully** to ensure all charges, checks, or withdrawals were authorized.
- **Guard your mail from theft.** If you have the type of mailbox with a flag to signal that the box contains mail, do not leave bill payment envelopes in your mailbox with the flag up. Instead, deposit them in a post office collection box or at the local post office. Promptly remove incoming mail.
- **Order copies of your credit report** from each of the three major credit bureaus once a year to ensure that they are accurate. The law permits the credit bureaus to charge \$8.50 for a copy of the report (unless you live in a state that requires the credit bureaus to provide you with one free copy of your report annually).
- **If you prefer not to receive preapproved offers of credit**, you can opt out of such offers by calling (888) 5 OPT OUT.
- **If you want to remove your name from many national direct mail lists**, send your name and address to:
DMA Mail Preference Service
P.O. Box 9008
Farmingdale, NY 11735-9008
- **If you want to reduce the number of telephone solicitations** from many national marketers, send your name, address, and telephone number to:
DMA Telephone Preference Service
P.O. Box 9014
Farmingdale, NY 11735-9014