COMMON WAYS ID THEFT HAPPENS:

Skilled identity thieves use a variety of methods to steal your personal information, including:

1. Dumpster Diving. They rummage through trash looking for bills or other paper with your personal information on it.
2. Skimming. They steal credit/debit card numbers by using a special storage device when processing your card.
3. Phishing. They pretend to be financial institutions or companies and send spam or pop-up messages to get you to reveal your personal information.
4. Social Engineering. They elicit personal information from you in person, over the telephone or via the Internet.
5. Changing Your Address. They divert your billing statements to another location by completing a "change of address" form.
6. "Old-Fashioned" Stealing. They steal wallets and purses; mail, including bank and credit card statements; pre-approved credit offers; and new checks or tax information. They steal personnel records from their employers, or bribe employees who have access.

OFFICE OF PROTECTIVE INTELLIGENCE
UNITED STATES MARSHAL

To learn more about ID theft and how to deter, detect, and defend against it, visit www.ftc.gov/idtheft.

The U.S. Marshals Service coordinated with the Federal Trade Commission to produce this publication.

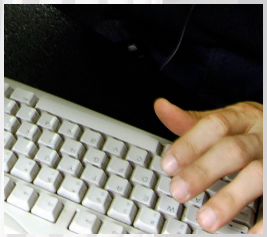
U.S. Department of Justice
United States Marshals Service
Washington, DC 20530-0001

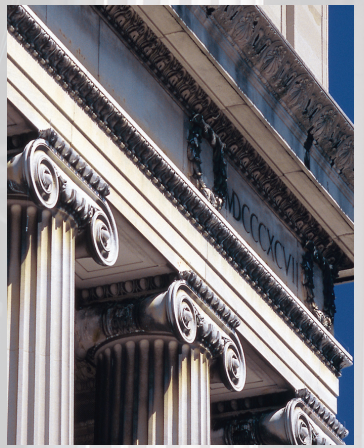
USMS Pub. 201
Rev. 04/2016

U.S. Department of Justice
United States Marshals Service
Judicial Security Division

AVOIDING IDENTITY THEFT

FOR THE FEDERAL JUDICIARY





DETER

Identity theft is a serious crime. It occurs when your personal information is stolen and used without your knowledge to commit fraud or other crimes. Identity theft can cost you time and money. It can destroy your credit and ruin your good name.

Deter identity thieves by safeguarding your information.

- Shred financial documents and paperwork with personal information before you discard them.
- Protect your Social Security number. Don't carry your Social Security card in your wallet or write your Social Security number on a check. Give it out only if absolutely necessary or ask to use another identifier.
- Don't give out personal information on the phone, through the mail, or over the Internet unless you know who you are dealing with.
- Never click on links sent in unsolicited emails; instead, type in a web address you know. Use firewalls, anti-spyware, and anti-virus software to protect your home computer; keep them up-to-date. Visit OnGuardOnline.gov for more information.
- Don't use an obvious password like your birth date, your mother's maiden name, or the last four digits of your Social Security number.
- Keep your personal information in a secure place at home, especially if you have roommates, employ outside help, or are having work done in your house.
- Do not sign up for contests that require your address and phone number or provide your phone number when making purchases.

DETECT

Detect suspicious activity by routinely monitoring your financial accounts and billing statements.

Be alert to signs that require immediate attention:

- Bills that do not arrive as expected.
- Unexpected credit cards or account statements.
- Denials of credit for no apparent reason.
- Calls or letters about purchases you did not make.

Inspect:

- Your credit report. Credit reports contain information about you, including what accounts you have and your bill paying history.
- The law requires the major nationwide consumer reporting companies–Equifax, Experian, and TransUnion–to give you a free copy of your credit report each year if you ask for it.
- Visit www.AnnualCreditReport.com or call 1-877-322-8228, a service created by these three companies, to order your free credit reports each year. It is recommended that you use this website every four months, selecting a different credit company each time. You also can write: Annual Credit Report Request Service, P.O. Box 105283, Atlanta, GA 30348-5283.
- Your financial statements. Review financial accounts and billing statements regularly, looking for charges you did not make.

DEFEND

Defend against ID theft as soon as you suspect it.

- Place a "Fraud Alert" on your credit reports, and review the reports carefully. The alert tells creditors to follow certain procedures before they open new accounts in your name or make changes to your existing accounts. The three nationwide consumer reporting companies have toll-free numbers for placing an initial 90-day fraud alert; a call to one company is sufficient:
  - Equifax: 1-888-766-0008
  - Experian: 1-888-EXPERIAN (397-3742)
  - TransUnion: 1-800-680-7289

  Placing a fraud alert entitles you to free copies of your credit reports. Look for inquiries from companies you haven't contacted, accounts you didn't open, and debts on your accounts that you can't explain.
- Close accounts. Close any accounts that have been tampered with or established fraudulently.
  - Call the security or fraud departments of each company where an account was opened or changed without your okay. Follow up in writing, with copies of supporting documents.
  - Use the ID Theft Affidavit at ftc.gov/idtheft to support your written statement.
  - Ask for verification that the disputed account has been closed and the fraudulent debts discharged.
  - Keep copies of documents and records of your conversations about the theft.
- File a police report. File a report with law enforcement officials to help you with creditors who may want proof of the crime.
- Report the theft to the Federal Trade Commission. Your report helps law enforcement officials across the country in their investigations.
  - Online: ftc.gov/idtheft
  - By phone: 1-877-ID-THEFT (438-4338) or TTY, 1-866-653-4261
  - Notify your local police department
- Notify your local U.S. Marshals Office.