Get back your good name.

In 2006, more than 8.9 million adults were victims of

IDENTITY CRIME.

Clear Your Good Name After Identity Crime

You suspect that someone is using your name and personal identification information for unlawful purposes. This kit can help you resolve your identity crime case and clear your name.

What Is Identity Crime?

Identity crime is the illegal use of another's personal information, such as credit card numbers, social security number, or driver's license number to commit fraud or other crimes. Criminals can obtain your personal identification information in any number of ways: stealing your purse or wallet, posing as bank representatives to trick you into revealing your account numbers over the phone, burglarizing your home to find financial documents, digging through your trash in search of preapproved credit card offers. The criminals use the information to drain your bank accounts, spend your available credit, apply for new credit in the your name, and even impersonate you to get jobs. Identity crime can go undetected for days, months, or even years, and it can leave you with ruined credit and a criminal record.

In partnership with:

Bank of America

What should I do if I become a victim?

What Should I Do If I Become A Victim?

Navigating through the system as an identity crime victim can be a lengthy and confusing process. As you contact law enforcement, creditors, and financial institutions, keep track of the actions you take and maintain a record of your progress. In the back of this kit, you will find a chart to help with your record keeping.

As soon as you become aware that someone has used your information to commit a crime, you should immediately take some basic steps to prevent additional crimes and begin repairing the damage to your good name. As you contact law enforcement agencies, creditors, and financial institutions, keep track of the actions you take and maintain a record of your progress. For a copy of the "Chart Your Course of Action" spreadsheet, visit www.ftc.gov/bcp/edu/resources/forms/chart-course-action.pdf.

Obtain a copy of your credit report:

Fraud victims are entitled to a free credit report. Carefully review the entire credit reporting record. Report any errors or actions that are suspect or fraudulent to all three of the credit reporting agencies:

Equifax
P.O. Box 740241
Atlanta, GA 30374-0241

To order your report:
800.685.1111

To report fraud:
800.525.6285

TDD: 800.255.0056

TransUnion
Fraud Victim Assistance
P.O. Box 6790
Fullerton, CA 92634-6790
Email: fvad@transunion.com

To order your report:
800.888.4213

To report fraud:
800.680.7289

TDD: 877.553.7803

Experian (formerly TRW)
P.O. Box 9532
Allen, TX 75013

To order your report:
888.EXPERIAN (397.3742)

To report fraud:
888.EXPERIAN (397.3742)

TDD: 800.972.0322

Report the incident to law enforcement:

Report identity crime to both the law enforcement agency that has jurisdiction where you live and the law enforcement agency that has jurisdiction where you believe the crime occurred. The address and telephone number of the local police department can be found in your local telephone directory. Once you have filed a report with police, request a copy of the report so that it will be available to send to credit reporting agencies and creditors.

When you file the report, provide as much documentation as possible, including copies of debt collection letters, credit reports and your notarized ID Theft Affidavit which can be found online at www.ftc.gov/bcp/conline/pubs/credit/affidavit.pdf.

Notify all credit card companies, creditors, banks, and financial institutions:

Call all credit card companies, creditors, banks, and other financial institutions where you have accounts that may have been affected or where an account may have been created in your name, without your knowledge, and ask them to help you take the following steps:

1. Request that those accounts be processed as "account closed at consumer's request."

2. Get replacement cards with new account numbers.

3. Stop payments on any checks or withdrawal drafts that are suspect.

4. Change any passwords and PINs on the accounts, including any automated teller machine (ATM) accounts with banks, savings institutions, other financial service entities, credit cards, online entities, and merchants.

5. Be sure your new password does not include your mother's maiden name, your birth date, any portion of your social security number or any other easily obtained passwords. Follow up all telephone contacts with a written confirmation.

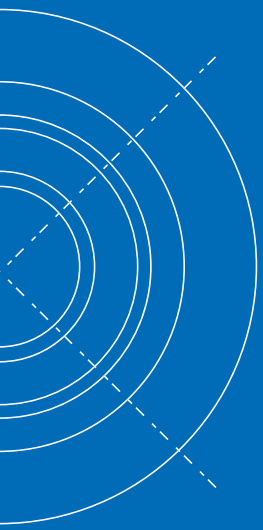
6. Follow up all telephone contacts with a written confirmation.

Notify all of the credit reporting agencies and put an alert on your accounts:
Report identity crime, and the theft of any credit cards or credit card numbers, to each credit reporting agency (contact information for the agencies is on page three of this booklet). Request that all your accounts be flagged with the appropriate fraud alert. There are two types of fraud alert: an initial alert and an extended alert.

Initial fraud alert:
An initial alert stays on your credit report for at least 90 days. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been a victim of identity crime. An initial alert is appropriate if your wallet has been stolen or if you have been taken in by a telephone or e-mail scam. When you place an initial fraud alert on your credit report, you are entitled to one free credit report from each of the three nationwide credit reporting agencies.

Extended fraud alert:
An extended alert stays on your credit report for seven years. You can have an extended alert placed on your credit report if you have been a victim of identity crime and you provide the credit reporting agencies with an identity crime report. When you place an extended alert on your credit report, you are entitled to two free credit reports within 12 months from each of the three nationwide credit reporting agencies. In addition, the consumer reporting companies will remove your name from marketing lists for prescreened credit offers for five years unless you ask them to put your name back on the list before the end of that time.

To place either of these alerts on your credit report, or to have them removed, you will be required to provide appropriate proof of your identity: that may include your name, address, social security number, and other personal information requested by the credit reporting agencies.



When a business sees the alert on your credit report, it must verify your identity before issuing you credit. As part of this verification process, the business may try to contact you directly. This may cause some delays if you are trying to obtain credit. To compensate for possible delays, you may wish to include a cell phone number, where you can be reached easily, in your alert. Remember to keep all contact information in your alert current.

Consider putting a security freeze on your credit report:

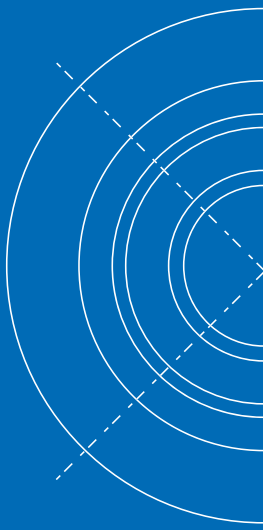
You may want to put a security freeze on your credit report with each credit reporting agency. A security freeze means that your credit report or credit score cannot be shared with others, such as potential creditors, without your authorization. This can help prevent further identity crime because most businesses will not open credit accounts without first checking your credit report. If someone tries to change certain information in a frozen credit report (like your name, address, birth date, or social security number), the credit reporting agency must send written confirmation of the change to you within 30 days. Each credit reporting agency may charge you up to $10 for security freezes, but there is no fee for an identity crime victim who provides a valid police report upon request. (The amount of the fee is subject to a yearly CPI adjustment). To put a security freeze on your credit report, send a written request by certified mail to the credit reporting agencies at the addresses on the following page, with proper identification and with the required fee. You may want to call each credit reporting agency, or visit its Web site, to confirm the amount of the fee and any special information you need to include with your request.

The credit reporting agency must place the freeze within 10 business days of receiving your request and send you a password or personal identification number (PIN) to use for making changes to the security freeze.

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
800.685.1111
www.equifax.com

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
888.397.3742
www.experian.com

TransUnion Security Freeze
P.O. Box 6790
Fullerton, CA 92834-6790
888.909.8872
www.transunion.com



You can allow access to your credit report for a specific period of time after you have placed a security freeze (for obtaining credit, or for a potential employer or for any other reason), or you can permanently remove the freeze. To do so, you must contact each credit reporting agency from which you want to temporarily lift or remove the freeze, and provide proper identification and the fee. Again, you may want to call the credit reporting agency or visit its Web site for specific information about temporarily lifting a freeze. Be sure that you make the request ahead of time, because the credit bureau has three business days to comply with your request.

Notify check verification companies:

Contact the major check verification companies at the numbers listed below if someone has stolen your personal checks or if you believe someone has set up bank accounts in your name. Inform the verification companies that you are an identity crime victim.

CheckRite: 800.234.7800
ChexSystems: 800.428.9623 (closed checking accounts)
CrossCheck: 800.552.1900
Equifax: 800.437.5120
International Check Services: 800.631.9656
National Processing Company (NPC): 800.526.5380
SCAN: 800.262.7771
TeleCheck: 800.710.9898

Notify your utility and service provider companies:

Notify your service providers (local telephone, long-distance telephone, cell phone, cable or satellite television, Internet, electric power, gas, and water) of the identity crime and inform them that attempts may be made to open new service using your identification information. Request that any new request for service be confirmed with you and provide a telephone number and mailing address. Keep a copy of all of these requests.

Notify your local post office:

Notify your local U.S. postal inspector if you suspect an identity criminal has filed a change of your address with the post office or has used the mail to commit fraud. Find out what your address was changed to, and instruct the local postmaster for that address to forward all mail addressed to you to your correct address. You may also need to talk with the mail carrier on the route where fraudulent mail is being sent. Confirm all telephone conversations in writing. To obtain the telephone number of your local post office, call 800.275.8777. The phone numbers for U.S. postal inspectors and post offices can also be obtained at www.usps.gov/postalinspectors.

Notify the Federal Trade Commission:

File a report of an identity crime and obtain assistance in restoring credit by writing to the Federal Trade Commission's Consumer Response Center at 600 Pennsylvania Avenue, NW, Washington, DC 20580, by calling 877.438.4338, or by visiting www.consumer.gov/idtheft and following instructions there. Another Web site maintained by the FTC, www.consumer.gov/idtheft/info.htm, offers helpful Internet links to other federal agencies and nonprofit organizations that provide assistance to victims of identity crime.

Notify the Social Security Administration:

Report a misuse or possible theft of your social security number to the Office of the Inspector General of the Social Security Administration by writing to that office at P.O. Box 17768, Baltimore, MD 21235, by calling the Social Security Administration Fraud Hotline at 800.269.0271, by sending a fax to 410.597.0018, by visiting www.ssa.gov/oig/hotline/ and following instructions there, or by sending an e-mail message to oig.hotline@ssa.gov.

Obtain a copy of your criminal history record:

Request a copy of your own criminal history record by calling or writing to the criminal records section of your state police department or state attorney general's office.

Notify your driver licensing agency:

Notify your state's driver licensing agency of the identity crime and ask it to place a flag on your driver record.

Notify the Federal Bureau of Investigation:

If the compromise of an identity is the result of, or otherwise connected to, an Internet or other online fraud, file an online fraud complaint with the FBI Internet Fraud Complaint Center at www.ifccfbi.gov.

Notify the U.S. State Department:

All identity crime victims, whether they have a passport or not, should notify the U.S. State Department of the identity crime. Victims should ask the State Department to confirm, by writing to the address you have provided, any application for a passport or changes of address. Online assistance is available from the State Department at www.travel.state.gov/passport/lost/us/us_848.html.

Notify other federal agencies as necessary:

Numerous federal agencies have jurisdiction over specific aspects of identity crime. If you experience a crime related to any of the following categories, contact the agencies directly for help and information or to initiate an investigation.

Bank fraud:

If you are having trouble getting your financial institution to help you resolve your banking-related identity crime problems, including problems with bank-issued credit cards, contact the agency with the appropriate jurisdiction. If do not know which of the agencies listed below has jurisdiction over your institution, call your bank or visit www.ffiec.gov/enforcement.htm.

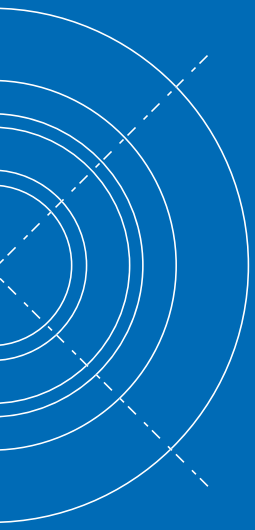
Federal Deposit Insurance
Corporation (FDIC)
800.934.3342
www.fdic.gov

Federal Reserve System
202.452.3693
www.federalreserve.gov

National Credit Union Association
703.518.6360
www.ncua.gov

Office of the Comptroller of Currency
800.613.6743
www.occ.treas.gov

Office of Thrift Supervision
202.906.6000
www.ots.treas.gov



Bankruptcy fraud:
If you believe someone has filed for bankruptcy in your name, write to the U.S. trustee in the region where the bankruptcy was filed. A list of the offices is available online at www.usdoj.gov/ust.

Investment fraud:
If you believe that an identity crime has tampered with your securities investments or a brokerage account, immediately report it to your broker or account manager or the U.S. Securities and Exchange Commission (SEC). You can file a complaint with the SEC online at www.sec.gov/complaint.shtml.

Cellular and long-distance phone fraud:
If you are having trouble getting fraudulent phone charges removed from your account or getting an unauthorized account closed, call the Federal Communications Commission (FCC) at 888.CALL.FCC (888.225.5322). File a complaint online at www.fcc.gov.

Tax fraud:
If you believe someone has assumed your identity to file federal income tax returns or to commit other tax fraud, call the Internal Revenue Service (IRS) at 800.829.0433 or visit www.treas.gov/irs/ci.

Stay alert:
Once resolved, most cases of identity crime stay resolved. Nevertheless, some victims have recurring problems. To help stay on top of the situation, continue to monitor your credit reports and read your financial account statements promptly and carefully.

You may want to review your credit reports once every three months in the first year of the crime and once a year thereafter. And stay alert for other signs of identity crime listed on the next page.

1. Failing to receive bills or other mail. Follow up with creditors if your bills do not arrive on time. A missing bill could mean an identity criminal has taken over your account and changed your billing address to cover his tracks.
2. Receiving credit cards that you did not apply for.
3. Being denied credit, or being offered less favorable credit terms, like a high interest rate, for no apparent reason.
4. Getting calls or letters from debt collectors or businesses about merchandise or services you did not buy.

Getting your credit report and free credit reports:

A recent amendment to the Fair Credit Reporting Act requires each of the major nationwide credit reporting agencies to provide you with a free copy of your credit report, at your request, once every 12 months. To order your free annual report from one or all of the national consumer reporting companies, visit www.annualcreditreport.com, call 877.322.8228, or complete the Annual Credit Report Request Form and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You can print this form from www.ftc.gov/credit.

Other consumer rights to free reports:

Under federal law, you are entitled to a free report if a company takes adverse action against you, such as denying your application for credit, insurance, or employment and you request your report within 60 days of receiving notice of the action. The notice will give you the name, address, and phone number of the reporting company. You are also entitled to one free report a year if you are unemployed and plan to look for a job within 60 days, you are on welfare, or your report is inaccurate because of fraud. Otherwise, a credit reporting agency may charge you up to $9.50 for another copy of your report within a 12-month period. To buy a copy of your report, call a credit reporting agency or visit its Web site. See page three of this booklet for a complete listing.

Protecting the Real You and Only You.

The International Association of Chiefs of Police
515 N. Washington Street, Alexandria, VA 22314
Telephone: 1.800.843.4227
www.theiacp.org