Identity Theft: What to Do if It Happens to You

You apply for a credit card and get turned down because of a low credit score.
Yet you know that you've always paid your accounts on time.
A debt collector calls to demand payment on a six-month overdue account for a credit card you have never had.
You receive a credit card in the mail that you've never applied for.

What's happening? You could be a victim of identity theft, where an imposter is using your personal information. The identity thief could use your personal information for any of the following:

- They may call your credit card issuer to change the billing address on your credit card account. The imposter then runs up charges on your account. Because your bills are being sent to a different address, it may be some time before you realize there's a problem.
- They may open new credit card accounts in your name. When they use the credit cards and don't pay the bills, the delinquent accounts are reported on your credit report.
- They may establish phone or wireless service in your name.
- They may open a bank account in your name and write bad checks on that account.
- They may counterfeit checks or credit or debit cards, or authorize electronic transfers in your name and drain your bank account.
- They may file for bankruptcy under your name to avoid paying debits they've incurred under you name or to avoid eviction.
- They may buy a car by taking out an auto loan in your name.
- They may get identification such as a driver's license issued with their picture, in your name.
- They may get a job or file fraudulent tax returns in your name.
- They may give your name to the police during an arrest. If they don't show up for their court date, a warrant for arrest is issued in your name.

How did this happen? Identity Thieves get your personal information by a variety of ways:

- They get information from businesses or other institutions by:

  - stealing records or information while they're on the job
  - bribing an employee who has access to these records
  - hacking these records
  - conning information out of employees

- They may steal your mail, including bank and credit card statements, credit card offers, new checks, and tax information.
- They may rummage through your trash, the trash of businesses, or public trash dumps in a practice known as “dumpster diving.”
- They may get your credit reports by abusing their employer’s authorized access to them, or by posing as a landlord, employer, or someone else who may have a legal right to access your report.
- They may steal your credit or debit card numbers by capturing the information in a data storage device in a practice known as “skimming.” They may swipe your card for an actual purchase, or attach the device to an ATM machine where you may enter or swipe your card.
- They may steal your wallet or purse.
- They may steal personal information they find in your home.
- They may steal personal information from you through email or phone by posing as legitimate companies and claiming that you have a problem with your account. This practice is known as “phishing” online, or “pretexting” by phone.

This guide provides victims of identity theft with instructions on how to regain your financial health and who to contact for more help. You must act quickly and assertively to minimize the damage.

1. Notify credit bureaus. Immediately report the situation to the fraud units of the three credit reporting companies -- Experian (formerly TRW), Equifax, and TransUnion. When you notify one bureau that you are a victim of identity theft, it will notify the other two for you. Report that your identifying information is being used by another person to obtain credit fraudulently in your name. Ask that your file be flagged with a fraud alert and that creditors call you before extending credit. Consider using your cell phone number if you have a mobile telephone.

Equifax: P.O. Box 740241, Atlanta, GA 30374-0241. **Report fraud:** Call (800) 525-6285 and write to address above. TDD: (800) 255-0056 Web: www.equifax.com	**Experian:** P.O. Box 9532 Allen, TX 75013. **Report fraud:** Call (888) EXPERIAN (888-397-3742) and write to address above. TDD: Use relay to fraud number above. Web: www.experian.com	**TransUnion:** P.O. Box 6790, Fullerton, CA 92834-6790. **Report fraud:** (800) 680-7289 and write to address above. TDD: (877) 553-7803 E-mail (fraud victims only): fvad@transunion.com Web: www.transunion.com

Under new provisions of the Fair Credit Reporting Act (FCRA, §605A) you can place an initial fraud alert for only 90 days. The credit bureaus will then mail you a notice of your rights as an identity theft victim. Once you receive it, write each of the three bureaus immediately to request two things: (1) a free copy of your credit report, and (2) an extension of the fraud alert to seven years. You may request that only the last four digits of your Social Security number (SSN) appear on the credit report. *You must include an identity theft report (police report) with your letter in order to establish the seven-year alert.* You may cancel fraud alerts at any time.

In all communications with the credit bureaus, you will want to refer to the unique number assigned to your credit report and use certified, return receipt mail. Be sure to save all credit reports as part of your fraud documentation.

Once you have received your three credit reports, examine each carefully. Report fraudulent accounts and erroneous information in writing to both the credit bureaus *and* the credit issuers following the instructions provided with the credit reports. The Federal Trade Commission's identity theft guide provides a sample letter to send to the credit bureaus requesting that fraudulent accounts be blocked. http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt04.pdf

Once you notify the credit bureaus about fraudulent accounts, the bureau is required to block that information from future reports. The bureau must also notify the credit grantor of the fraudulent account. (FCRA, §605B) Ask the credit bureaus for names and phone numbers of credit grantors with whom fraudulent accounts have been opened if this information is not included on the credit report.

In addition, instruct the credit bureaus in writing to remove *inquiries* that have been generated due to the fraudulent access. You may also ask the credit bureaus to notify those who have received your credit report in the last six months in order to alert them to the disputed and erroneous information (two years for employers).

1a. Monitor your credit reports. *Be aware that these measures may not entirely stop new fraudulent accounts from being opened by the imposter.* Credit issuers do not always pay attention to fraud alerts, even though the law now requires it. Once you have received your first free copy of your credit report *and* have requested that the fraud alert be extended to seven years, follow up in a few months with a request for your second free copy, which federal law enables you to receive. In addition, every consumer, whether or not a victim of identity theft, can receive one free report every twelve months from each of the three national credit bureaus. (FCRA §612) For more on free credit reports, see www.ftc.gov/bcp/menus/consumer/credit/rights.shtm as well as www.annualcreditreport.com.

Laws in several states give individuals additional opportunities to obtain free credit reports. Missouri State Statute allows for one free annual credit report from each of the three credit bureaus. See the Federal Trade Commission's (FTC) list of states that offer a free credit report or a report at reduced rates, even if you are not a victim of identity theft.
http://www.consumer.gov/idtheft/

1b. Security freeze. A "security freeze" is stronger than a fraud alert because it prevents anyone from accessing your credit file for any reason until and unless you instruct the credit bureaus to unfreeze your report. A security freeze is authorized in Missouri under State Statute 407.1400 RSMo. The security freeze is also available in several other states, according to the National Conference of State Legislatures. www.ncsl.org/programs/banking/SecurityFreeze_2005.htm

2. Law enforcement. Report the crime to your local police or sheriff's department. You might also need to report it to police department(s) where the crime occurred, if it's somewhere other than where you live. Give them as much documented evidence as possible. *Make sure the police report lists the fraud accounts. Get a copy of the report, which is called an "identity theft report" under the FCRA.* Keep the phone number of your investigator handy and give it to creditors and others who require verification of your case. Credit card companies and banks may require you to show the report in order to verify the crime.

3. Federal Trade Commission. Report the crime to the Federal Trade Commission. Include your police report number. They share such information with investigators nationwide who are fighting identity theft.

- Call the FTC's Identity Theft Hotline: (877) IDTHEFT (877-438-4338)
- Or use its online identity theft complaint form: www.ftc.gov/ftc/cmplanding.shtm
- Or write: FTC Identity Theft Clearinghouse, 600 Pennsylvania Ave. N.W., Washington, DC 20580.

4. What to do with *new* credit accounts opened by the imposter. If your credit report shows that the imposter has opened new accounts in your name, contact those creditors immediately by phone and in writing. Recent amendments to the FCRA (§623(6)(B)) allow you to prevent businesses from reporting fraudulent accounts to credit bureaus.
Creditors will likely ask you to fill out fraud affidavits. The FTC provides a uniform affidavit form that most creditors accept (www.ftc.gov/bcp/edu/resources/forms/affidavit.pdf). No law requires affidavits to be notarized at your own expense. You may choose to substitute witness signatures for notarization if creditors require verification of your signature.
Ask the credit grantors in writing to furnish you and your investigating law enforcement agency copies of the documentation, such as the fraudulent

application and transaction records. Federal law gives you the right to obtain these documents. (FCRA § 609(e).

A victim of identity theft must provide a copy of the FTC affidavit or another affidavit acceptable to the business, plus government-issued identification, and a copy of an "identity theft report" (police report) in order to obtain the documents created by the imposter. The business must provide copies of these records to the victim within 30 days of the victim's request at no charge. The law also allows the victim to authorize a law enforcement investigator to get access to these records.

When you have resolved the fraudulent account with the creditor, ask for a letter stating that the company has closed the disputed account and has discharged the debts. Keep this letter in your files. You may need it if the account reappears on your credit report.

You must also notify the credit bureaus about the fraudulent accounts. Instructions are provided in section 1 above.

5. Handling problems with your existing credit or debit accounts. *If your existing credit or debit accounts* have been used fraudulently, report it in writing immediately to the credit card company. Get replacement cards with new account numbers. In addition to phoning the credit card company regarding the fraud, you will need to *follow up in writing* and will likely be asked to provide a fraud affidavit or a dispute form. Send the letter to the address given for "billing inquiries," *not* the address for sending payments. Carefully monitor your mail and bills for evidence of new fraudulent activity. Report it immediately. *Add passwords to all accounts*. These should not be your mother's maiden name or any word that is easily guessed.

6. Debt collectors. If debt collectors attempt to require you to pay the unpaid bills on fraudulent accounts, ask for the name of the collection company, the name of the person contacting you, phone number, and address. Tell the collector that you are a victim of fraud and are not responsible for the account. Ask the collector for the name and contact information for the referring credit issuer, the amount of the debt, account number, and dates of the charges. Ask if they need you to complete their fraud affidavit form or if you can use the Federal Trade Commission affidavit. *Follow up in writing to the debt collector* explaining your situation. Ask that they confirm in writing that you do not owe the debt and that the account has been closed. Under new provisions in the FCRA, a debt collector must notify the creditor that the debt may be a result of identity theft (§615(g)). The FCRA also prohibits the sale or transfer of a debt caused by identity theft. (§615(f))

7. Check and banking fraud. *If you have had checks stolen* or bank accounts set up fraudulently, ask your bank to report it to ChexSystems, a consumer

reporting agency that compiles reports on checking accounts. Also, place a security alert on your file (see web address below).
Your bank branch should be able to provide you with a fraud affidavit. Put stop payments on any outstanding checks that you are unsure of. Cancel your checking account and other affected accounts and obtain new account numbers. Give the bank a password for your account (not mother's maiden name, Social Security number, date of birth, sequential numbers, or any other easily guessed words).

- If you subsequently have trouble opening new bank accounts, contact ChexSystems to correct your file: Phone: (800) 428-9623. Fax: (602) 659-2197
- Web: www.chexhelp.com
- To place a security alert on your ChexSystems report: https://www.consumerdebit.com/consumerinfo/us/en/chexsystems/theftaffidavit/index.htm
- Write: ChexSystems Inc., Attn: Consumer Relations, 7805 Hudson Rd., Suite 100, Woodbury, MN 55125.

If your own checks are rejected at stores where you shop, contact the check verification company that the merchant uses. The major ones are listed here.

Certegy (was Equifax)	(800) 437-5120	www.certegy.com
SCAN	(800) 262-7771	
TeleCheck For annual file disclosure Fraud, ID Theft Department	(800) 710-9898 (800) Telecheck (800) 927-0188	www.telecheck.com
International Check Services	(800) 526-5380	
CrossCheck	(800) 843-0760	www.cross-check.com

Under a new federal law, you now have a right to obtain any reports that these companies compile about you. For ChexSystems and any of the check verification companies listed here that you have had to contact as a result of your identity theft situation, we recommend that you request a copy of your file once a year. Make sure your file has been corrected. If not, you will find it difficult to open up new bank accounts and/or write checks where you shop. Visit the web sites listed above to learn how to order your free annual reports.

Where to Find Help

If you have trouble getting a financial institution to help you resolve your banking-related identity theft problems, including problems with bank-issued credit cards, contact the agency that oversees your bank (see list below). If you're not sure which of these agencies is the right one, call your bank or visit the National Information Center of the Federal Reserve System at www.ffiec.gov/nic/ and click on "Institution Search."

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

The FDIC supervises state-chartered banks that are not members of the Federal Reserve System, and insures deposits at banks and savings and loans. Call the FDIC Consumer Call Center toll-free: 1-800-934-3342; or write: Federal Deposit Insurance Corporation, Division of Compliance and Consumer Affairs, 550 17th Street, NW, Washington, DC 20429.

Federal Reserve System (Fed) – www.federalreserve.gov

The Fed supervises state-chartered banks that are members of the Federal Reserve System.
Call: 202-452-3693; or write: Division of Consumer and Community Affairs, Mail Stop 801, Federal Reserve Board, Washington, DC 20551; or contact the Federal Reserve Bank in your area. The Reserve Banks are located in Boston, New York, Philadelphia, Cleveland, Richmond, Atlanta, Chicago, St. Louis, Minneapolis, Kansas City, Dallas, and San Francisco.

National Credit Union Administration (NCUA) – www.ncua.gov

The NCUA charters and supervises federal credit unions and insures deposits at federal credit unions and many state credit unions.
Call: 703-518-6360; or write: Compliance Officer, National Credit Union Administration, 1775 Duke Street, Alexandria, VA 22314.

Office of the Comptroller of the Currency (OC) – www.occ.treas.gov

The OCC charters and supervises national banks. If the word "national" appears in the name of a bank, or the initials "N.A." follow its name, the OCC oversees its operations.
Call toll-free: 1-800-613-6743 (business days 9:00 a.m. to 4:00 p.m. CST); fax: 713-336-4301; or write: Customer Assistance Group, 1301 McKinney Street, Suite 3710, Houston, TX 77010.

Office of Thrift Supervision (OTS) – www.ots.treas.gov

The OTS is the primary regulator of all federal, and many state-chartered, thrift institutions, including savings banks and savings and loan institutions.
Call: 202-906-6000; or write: Office of Thrift Supervision, 1700 G Street, NW, Washington, DC 20552.

8. ATM cards. *If your ATM or debit card has been stolen or compromised*, report it immediately. Contact your bank branch and fill out a fraud affidavit. Get a new card, account number, and password. Do not use your old password. Monitor your account statements. *You may be liable if fraud is not reported quickly.* Start with a phone call and immediately follow up in writing. Be sure to read the debit card contract for information about liability. Some cards are better protected in cases of fraud than others.

ATM and debit card transactions are subject to the Electronic Fund Transfer Act. (15 USC §1693) Even if you are a victim of identity theft, your liability for charges can increase the longer the crime goes unreported. For more on EFTA, see the Federal Reserve Board's guide, www.federalreserve.gov/pubs/consumerhdbk/electronic.htm.

9. Fraudulent change of address or mail theft. Notify the local Postal Inspector if you suspect an identity thief has filed a change of your address with the post office or has used the mail to commit fraud. Find out where fraudulent credit cards were sent. Notify the local Postmaster for that address to forward all mail in your name to your own address. You may also need to talk with the mail carrier. Call the U.S. Postal Service to find the nearest Postal Inspector at (800) 275-8777 or visit its web site at http://postalinspectors.uspis.gov/

10. U.S. Secret Service. The U.S. Secret Service has jurisdiction over financial fraud. But, based on U.S. Attorney guidelines, it usually does not investigate individual cases unless the dollar amount is high or you are one of many victims of a fraud ring. To interest the Secret Service in your case, you may want to ask the fraud department of the credit card companies and/or banks to notify the Secret Service.

11. Social Security Number (SSN) misuse. The Social Security Administration (SSA) does *not* in most cases provide assistance to identity theft victims. But be sure to contact the SSA Inspector General to report Social Security benefit fraud, employment fraud, or welfare fraud.

- Social Security Administration online complaint form: www.socialsecurity.gov/oig
- SSA fraud hotline: (800) 269-0271
- By mail: SSA Fraud Hotline, P.O. Box 17768, Baltimore, MD 21235

As a last resort, you might try to change your number, although *we don't recommend it except for very serious cases*. The SSA will only change the number if you fit their fraud victim criteria.

If your SSN card has been stolen or lost, order a replacement. Complete the SSA's application available at www.socialsecurity.gov/online/ss-5.html, or by calling the SSA at (800) 772-1213, or by visiting your local SSA office. You will

need to provide the required documentation such as birth certificate and government ID at your local SSA office to get a replacement card.

12. Passports. Whether you have a passport or not, write the passport office to alert them to anyone ordering a passport fraudulently.

- U.S. Dept. of State, Passport Services, Consular Lost/Stolen Passport Section, 1111 19th St., NW, Suite 500, Washington, DC 20036.
- Website: www.travel.state.gov/passport/lost/lost_849.html

13. Phone service. Identity thieves often establish fraudulent wireless phone accounts, with monthly bills going unpaid. The imposter might also have opened local and long distance phone accounts. If you have learned that the imposter has obtained phone account(s) in your name, contact the phone company for information on how to report the situation. The steps that you take to clear your name with both the phone company and credit bureaus are much the same as with credit card accounts described above.
If your calling card has been stolen or there are fraudulent charges, cancel it and open a new account. For your own phone accounts, add a password that must be used any time your local, cell, and long distance accounts are changed.

If you're having trouble getting fraudulent phone charges removed from your account or getting an unauthorized account closed, contact the appropriate agency below:

- For local service, contact your state Public Utility Commission.
- For cellular phones and long distance, contact the Federal Communications Commission (FCC) at www.fcc.gov. The FCC regulates interstate and international communications by radio, television, wire, satellite, and cable. Call 1-888-CALL-FCC; TTY: 1-888-TELL-FCC; or write:

  Federal Communications Commission, Consumer Information Bureau
  445 12th Street, SW, Room 5A863, Washington, DC 20554.

  You can file complaints online at www.fcc.gov, or e-mail your questions to fccinfo@fcc.gov.

14. Student loans. If an identity thief has obtained a student loan in your name, report it in writing to the school that opened the loan. Request that the account be closed. Also report it to the U.S. Dept. of Education:

- Call U.S. Dept. of Education Inspector General's Hotline: (800) MIS-USED (800-647-8733)
- Write: Office of Inspector General, U.S. Dept. of Education, 400 Maryland Ave., SW, Washington, DC 20202-1510.

Web: www.ed.gov/about/offices/list/oig/hotline.html?src=rt

15. Driver's license number misuse. You may need to change your driver's license number if someone is using yours as ID on bad checks or for other types of fraud. Call the Department of Revenue or Department of Motor Vehicles to see if another license was issued in your name. Put a fraud alert on your license if your state's DOR or DMV provides a fraud alert process. Go to your local DOR or DMV to request a new number. Fill out the office's complaint form to begin the investigation process. Send supporting documents with the completed form to the nearest DOR or DMV investigation office. In Missouri contact the Department of Revenue Criminal Investigation Bureau at 573-751-4689.

- Departments in other states: http://www.aamva.org/

16. False civil and criminal judgments. Sometimes victims of identity theft are wrongfully accused of crimes committed by the imposter. If you are wrongfully arrested or prosecuted for criminal charges, contact the police department and the court in the jurisdiction of the arrest. Also contact the Department of Justice and the FBI. Ask how to clear your name. If a civil judgment is entered in your name for your imposter's actions, contact the court where the judgment was entered and report that you are a victim of identity theft.

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 U.S. Trustee Programs' Regional Offices is available on the UST website (www.usdoj.gov/ust), or check the Blue Pages of your phone book under U.S. Government Bankruptcy Administration. The U.S. Trustee will make a criminal referral to law enforcement authorities if you provide appropriate documentation to substantiate your claim. The U.S. Trustee does not provide legal representation, legal advice, or referrals to lawyers. That means you may need to hire an attorney to help convince the bankruptcy court that the filing is fraudulent. When you or your attorney ask the bankruptcy court to dismiss the fraudulently filed bankruptcy case, you also should request that the bankruptcy court include in its order of dismissal facts that will help you repair your credit, including a statement that you did not file this bankruptcy case and that the case was filed by an imposter as the result of identity theft.

17. Tax Fraud. If an imposter files a fraudulent tax return in your name. The IRS is responsible for administering and enforcing tax laws. Identity fraud may occur as it relates directly to your tax records. Visit www.irs.gov and type in the IRS key word "Identity Theft" for more information.
If you have an unresolved issue related to identity theft, or you have suffered or are about to suffer a significant hardship as a result of the administration of the tax laws, visit the IRS Taxpayer Advocate Service website

www.irs.gov/advocate/ or call toll-free: 1-877-777-4778.

18. Other forms of identity theft. A deceased relative's information may be used to perpetrate identity theft.

19. Legal help. You may want to consult an attorney to determine legal action to take against creditors, credit bureaus, and/or debt collectors if they are not cooperative in removing fraudulent entries from your credit report or if negligence is a factor. Call the local Bar Association (www.abanet.org/premartindale.html), a Legal Aid office in your area (for low-income households), or the National Association of Consumer Advocates (www.naca.net) to find an attorney who specializes in consumer law, the Fair Credit Reporting Act, and the Fair Credit Billing Act.
If you are a senior citizen or take care of a dependent adult, be sure to contact an elder law service or the nearest Aging and Independent Services program. Many district attorneys have an elder abuse unit with expertise in financial crimes against seniors. In Missouri contact the Missouri Department of Health and Senior Services at 573-751-6400.

20. Victim statements. If the imposter is apprehended by law enforcement and stands trial and/or is sentenced, write a victim impact letter to the judge handling the case. Contact the victim-witness assistance program in your area for further information on how to make your voice heard in the legal proceedings.

21. Keep good records. In dealing with the authorities and financial companies, *keep a log* of all conversations, including dates, names, and phone numbers. Note time spent and expenses incurred in case you are able to seek restitution in a later judgment or conviction against the thief. You may be able to obtain tax deductions for theft-related expenses (26 U.S.C. §165(e) -- consult your accountant). Confirm conversations in writing. Send correspondence by certified mail, return receipt requested. Keep copies of all letters and documents. Tips for organizing your case, and other useful information for victims, can be found in the Federal Trade Commission's guide, *Take Charge*, at www.consumer.gov/idtheft.

22. Dealing with emotional stress. Psychological counseling may help you deal with the stress and anxiety commonly experienced by victims. Know that you are not alone. Contact the Identity Theft Resource Center for information on how to network with other victims and deal with the impact of this crime. www.idtheftcenter.org

23. Making change. Write to your state and federal legislators. Demand stronger privacy protection and prevention efforts by creditors and credit bureaus.

24. Don't give in. Do not pay any bill or portion of a bill that is a result of fraud. Do not cover any checks that were written or cashed fraudulently. Do not file for

bankruptcy. Your credit rating should not be permanently affected. No legal action should be taken against you. If any merchant, financial company or collection agency suggests otherwise, restate your willingness to cooperate, but don't allow yourself to be coerced into paying fraudulent bills. Report such attempts to government regulators immediately.

Other Useful Tips

If you are in the military, place an active duty alert on your credit report
When you are away from your usual duty station, you can place an active duty alert on your three credit reports as an extra protection against identity theft. The alert remains on your credit reports for 12 months. Contact the fraud departments for the three credit bureaus. Those phone numbers are provided in section 1 above.

Order your free credit report
Whether or not you are a victim of identity theft, take advantage of your free annual credit reports, now a requirement of federal law.

- Phone: (877) 322-8228
- Web: www.annualcreditreport.com

Opt out of pre-approved offers of credit for all three credit bureaus

- Call (888) 5OPTOUT (888-567-8688). You may choose a two-year opt-out period or permanent opt-out status.
- Or opt-out online, www.optoutprescreen.com.

Remove your name from mail marketing lists (Direct Marketing Association)

- Write: Mail Preference Service, P.O. Box 643, Carmel, NY 10512.

Web: www.dmachoice.org. Online opt-out program costs a monetary fee. It is free by mail.

Remove your phone number(s) from telemarketing lists

- Phone the FTC's Do Not Call Registry: (888) 382-1222
- Online registration: www.donotcall.gov

Order your earnings report from the Social Security Administration

- Order your Personal Earnings and Benefits Estimate Statement if you suspect an identity thief has used your SSN for employment: (800) 772-1213. The SSA automatically mails it to individuals three months before the birthday each year. www.ssa.gov/online/ssa-7004.html

- For information on reporting fraud to the SSA, read tip 11 above.

Resources

Federal Trade Commission (FTC)

- Read its guide, *Take Charge: Fighting Back Against Identity Theft*, http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt04.shtm
- Online information and complaint form: www.consumer.gov/idtheft
- Identity Theft Hotline: (877) IDTHEFT (877-438-4338)
- Write: FTC Identity Theft Clearinghouse, 600 Pennsylvania Ave. N.W., Washington, DC 20580

Identity Theft Resource Center (ITRC), P.O. Box 26833, San Diego, CA 92196. The ITRC offers many guides for victims and in-depth assistance by phone: (858) 693-7935. Web: www.idtheftcenter.org. E-mail: itrc@idtheftcenter.org

U.S. PIRG and the State PIRGs

- Read its model legislation for identity theft prevention, www.pirg.org/consumer/credit/model.htm

Identity Theft Survival Kit, Mari Frank, Esq. Author of *From Victim to Victor: A Step-by-Step Guide for Ending the Nightmare of Identity Theft* and *Safeguard Your Identity: Protect Yourself with a Personal Privacy Audit*. Phone: (800) 725-0807. Web: www.identitytheft.org.

U.S. Dept. Of Justice. The DOJ prosecutes some identity theft cases. Visit its web site for identity theft information: www.usdoj.gov/criminal/fraud/websites/idtheft.html

Internet Crime Complaint Center. Report cases involving online fraud and phishing. Web: www.ic3.gov/default.aspx

Webster Groves Police Department
Identity Crime Incident Checklist

First Name: _____

Middle Name: _____

Last Name: _____

Social Security Number: _____

Driver's License Number: _____

Date of Birth: _____

Home Address: _____

Home Telephone Number: _____

Cell Phone Number:_____

E-Mail Address: _____

Employer: _____

Work Address: _____

Work Telephone Number: _____

1. How did the Victim become aware of the identity crime? (check all that apply)

_____ found fraudulent charges on my credit card bill

_____ found fraudulent charges on my cellular phone bill

_____ received bills for an account(s) I did not open

_____ found irregularities on my credit report

_____ was contacted by a creditor demanding payment

_____ was contacted by a bank's fraud department regarding charges

_____ was denied a loan

_____ was denied credit

_____ was arrested, had a warrant issued, or a complaint filed in my name for a crime I did not commit.

_____ was sued for a debt I did not incur

_____ was not receiving bills regularly for a legitimate account

_____ was denied employment

_____ had my driver's licenses suspended for actions I did not commit

_____ received a legal filing I did not file, such as a bankruptcy

_____ other

3. What date did the Victim first become aware of the identity crime?

4. When did the fraudulent activity begin?

5. What is the full name, address, birth date, and other identifying information that the fraudulent activity was made under?

6. Please list all fraudulent activity that the Victim is aware of to date, with the locations and addresses of where fraudulent applications or purchases were made (retailers, banks, etc.).

7. What documents and identifying information were stolen and/or compromised?

_____ credit card(s) (List bank(s) issuing credit card)

_____ ATM card (List bank issuing ATM card)

_____ checks and/or checking account number (List bank issuing checks)

_____ savings account passbook or number (List bank holding savings account)

_____ brokerage or stock accounts (List banks and/or brokers)

_____ driver's license or license number (List state issuing license)

_____ state identity card or identity number (List state issuing card)

_____ social security card or number

_____ birth certificate (List state and municipality issuing birth certificate):

_____ resident alien card, green card, or other immigration documents

_____ bank account passwords or "secret words", such as mother's maiden name

_____ Other

_____ Unknown

8. What identity crimes have been committed?

_____ making purchase(s) using my credit cards or credit card numbers without authorization

_____ opening new credit card accounts in my name

_____ opening utility and/or telephone accounts in my name

_____ unauthorized withdrawals from my bank accounts

_____ opening new bank accounts in my name

_____ taking out unauthorized loans in my name

_____ unauthorized access to my securities or investment accounts

_____ obtaining government benefits in my name

_____ obtaining employment in my name

_____ obtaining medical services or insurance in my name

_____ check fraud

_____ passport/visa fraud

_____ other

9. What circumstances and activities have occurred in the last six months (include activities done by the Victim and on Victim's behalf by a member of his family or a friend)?

_____ carried Social Security Card in a wallet

_____ carried my bank account passwords, PINs, or codes in a wallet

_____ gave out Social Security Number (To whom?)

_____ mail was stolen (When? (approximately)

_____ went away and mail was held at the post office or collected by someone else

_____ traveled to another location outside home area (business or pleasure)

_____ mail was diverted from home (either by forwarding order or in a way unknown)

_____ did not receive a bill as usual (i.e., a credit card bill failed to come in the mail)

_____ a new credit card was supposed to be sent but did not arrive in the mail as expected

_____ bills being paid were left in an unlocked mailbox for pickup by the postal service

_____ service people were in the home (From what company? When?)

_____ documentation with personal information was thrown in the trash without being shredded

_____ credit card bills, pre-approved credit card offers, or credit card "convenience" checks in Victim's name were thrown out without being shredded

_____ garbage was stolen or gone through

_____ ATM receipts and/or credit card receipts were thrown away without being shredded

_____ password or PIN was given to someone else

_____ home was burglarized

_____ car was stolen or broken into

_____ purse or wallet was stolen

_____ checkbook was stolen

_____ personal information was provided to a service business or non-profit (i.e., gave blood, donated money, took out insurance, or saw a financial planner)

_____ credit report was queried by someone claiming to be a legitimate business interest (Who?)

_____ applied for credit and/or authorized a business to obtain credit report (i.e., shopped for a new car, applied for a credit card, or refinanced a home)

_____ personal information is available on the Internet, such as in an "open directory," genealogy web site, or college reunion web site

_____ a legitimate purchase was made where Victim's credit card was out of sight

_____ personal information was given to a telemarketer or a telephone solicitor

_____ personal information was given to a door-to-door salesperson or charity fundraiser

_____ a charitable donation was made using personal information

_____ personal information was given to enter a contest or claim a prize that was won

_____ a new bank account or new credit card account was legitimately opened in the Victim's name

_____ re-financed house or property (Please List)

_____ a legitimate loan was applied for or closed in the Victim's name

_____ a legitimate lease was applied for or signed in the Victim's name

_____ legitimate utility accounts were applied for or opened in the Victim's name

_____ a license or permit was applied for legitimately in the Victim's name

_____ government benefits were applied for legitimately in the Victim's name

_____ name and personal information were mentioned in the press, such as in a newspaper, magazine, or on a web site

_____ online purchases were made using credit card (Through what company?)

_____ personal information was included in an e-mail

_____ released personal information to a friend or family member

For any items checked above, please, include as much detail as possible, explain the circumstances of the situation

10. How many purchases over the Internet (retailer or auction sites) have been made in last six months?

11. What Internet sites has Victim bought from?

12. In the last six months, whom has the Victim's Social Security Number been given to?

13. Do the Victim's checks have their Social Security Number or Driver's License Number imprinted on them?

_____ Yes. (Please list retailer names where checks have been tendered)
_____ No.

14. Has the Victim documented his Social Security Number or Driver's License Number on any checks in the last six months?
_____ Yes.
_____ No.

15. Does the Victim have any information on a suspect in this identity crime case?
_____ Yes.
_____ No.

16. Please list all the banks the Victim has accounts with.

17. Please list all the credit card companies and banks the Victim has credit cards with.

18. Please list all the financial institutions the Victim has loans, leases, and mortgages from.

19. Please list any merchants who the Victim has credit accounts with such as department stores, or retailers.

20. Please list any other financial institutions where fraudulent accounts were opened in the Victim's name or using their personal identifiers.

21. Please list any documents fraudulently obtained in the Victim's name (driver's licenses, social security cards, etc.)

22. Has the Victim requested a credit report from each of the three credit bureaus? If so, attach a copy to the report
_____ Equifax
_____ TransUnion
_____ Experian

23. Has the Victim contacted any financial institution, concerning either legitimate or fraudulently opened accounts? If yes, please document the following
_____ name of the financial institution
_____ phone number
_____ institution representative