Resources

Credit reporting bureaus:

Equifax: PO Box 740241
Atlanta, GA 30374

- Report Fraud: Call (866) 349-5191 and write to address above.
- Order a credit report: (800) 685-1111.
- Opt out of pre-approve offers of credit; (888) 5OPTOUT or (888) 567-8688.

Experian: PO Box 4500
Allen, TX 75013

- Report Fraud or Order Credit Report: (888) 397-3742
- Consumer Relations: (800) 916-8800 and write to Fraud Victim Assistance Division, PO Box 6790, Fullerton, CA 92834-6790

Trans Union: PO Box 390
Springfield, PA 19064

- Report Fraud: (800) 680-7289
- Consumer Relations: (800) 916-8800 and write to Fraud Victim Assistance Division, PO Box 6790, Fullerton, CA 92834-6790

Remember, if you have been the victim of credit fraud (15 USC ß1681j(b)) or are denied credit (15 USC ß1681j(c)(3)) you are entitled to a free credit report. If you are a victim of fraud, be sure to ask the credit bureaus for free copies. They will often provide them.

Social Security Administration:

- Report Fraud: (800) 269-0271
- Order your Earnings and Benefits Statement: (800) 772-1213

To remove your name from mail and phone lists:

- Direct Marketing Association
  www.dmachoice.org

To report fraudulent use of your checks:

- Federal Trade Commission: (877) 438-4338
- CrossCheck: (800) 843-0760
- Chexsystems: (800) 428-9623
- Cartegy Check Services: (800) 437-5120
- Telecheck: (800) 710-9898

Other useful resources:

- Federal Government Information Center: Call (800) 688-9889 for help in obtaining government agency phone numbers.
- Federal Trade Commission (877) FTC-HELP for help in any type of consumer complaint (105 PL 318,112 Stat. 3007 Section 5) (specifically identity theft and referrals to local law enforcement). FTC Consumer's Page: https://www.consumer.ftc.gov

Laws:

Federal

Identity Theft and Assumption Deterrence Act
Public Law 105-318, 112 Stat. 3007 (Oct. 30, 1998)
www.ftc.gov/enforcement/statutes

Fair Credit Reporting Act (FCRA) 15 U.S.C. ß 1681 et seq.
www.ftc.gov/enforcement/statutes

State of Illinois

Financial Identity Theft
720 ILCS 5/16G

Useful internet locations:

- Federal Trade Commission
  www.ftc.gov/
- Privacy Rights Clearinghouse
  www.privacyrights.org/Identity-Theft-Data-Breaches
- Identity Theft Resource Center
  www.idtheftcenter.org/
- Type "Identity Theft" into your web browser

This guide was adapted with permission from the Privacy Rights Clearinghouse, San Diego, California.

What to do if it happens to you

UIS POLICE DEPARTMENT
University of Illinois Springfield
One University Plaza, MS PDB 1
Springfield, Illinois 62703-5407
Phone: (217) 206-6690

This guide provides victims of identity theft with the major resources to contact. Victims themselves have the ability to assist greatly with resolving their case. It is important to act quickly and assertively to minimize the damage.

www.uis.edu/police/

UNIVERSITY OF ILLINOIS SPRINGFIELD

In dealing with the authorities and financial institutions, ***keep a log*** *of all conversations, including dates, times, names, and phone numbers. Note the time spent and any expenses incurred. Confirm conversations in writing. Send correspondence by certified mail (return receipt requested). Keep copies of all letters and documents.*

Once you discover you are a victim of identity theft you should notify the following:

1. Credit bureaus. Immediately call the fraud units of the three credit reporting companies--Experian, Equifax, and Trans Union. Report the theft of your credit cards or numbers. The phone numbers are provided at the end of this brochure. Ask that your account be flagged. Also, add a victim's statement to your report, up to 100 words. ("My ID has been used to apply for credit fraudulently. Contact me at (your telephone number) to verify all applications.") Be sure to ask how long the fraud alert is posted on your account, and how you can extend it if necessary. *Be aware that these measures may not entirely stop new fraudulent accounts from being opened by the imposter. Ask the credit bureaus in writing to provide you with a free copy every few months so you can monitor your credit report.* Ask the credit bureaus for names and phone numbers of credit grantors with whom fraudulent accounts have been opened. Ask the credit bureaus to remove the 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).

2. Creditors. Contact all creditors immediately with whom your name has been used fraudulently--by phone and in writing. Get replacement cards with new account numbers for your own accounts that have been used fraudulently. Ask that old accounts be processed as "account closed at consumer's request." (This is better than "card lost or stolen" when this statement is reported to credit bureaus, it can be interpreted as blaming you for the loss.) Carefully monitor your mail and credit card bills for evidence of new fraudulent activity. Report it immediately to credit grantors.

Creditors requirement to report fraud. You may be asked by banks and credit grantors to fill out and notarize fraud affidavits, which could become costly. The law does not require that a notarized affidavit be provided to creditors. A written statement and supporting documentation should be enough (unless the creditor offers to pay for the notary).

3. Law Enforcement. Report the crime to the law enforcement agency with jurisdiction in your case. Give them as much documented evidence as possible. Get a copy of your police report. Keep the report number of your police report 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 to verify the crime. Some police departments have been known to resist writing reports on such crimes. Prior to January 1st, 1998, the creditors (credit card companies, banks, etc.) were the only "legal" victims of Credit Fraud/Identity Theft. Some police departments have not yet received training in the new laws of Identity Theft. Be persistent!

4. Stolen Checks. If you have had checks stolen or bank accounts set up fraudulently, report it to the check verification companies. Put stop payments on any outstanding checks that you are unsure of. Cancel your checking and savings accounts and obtain new account numbers. Give the bank a secret password for your account (not your mother's maiden name).

5. ATM Cards. If your ATM card has been stolen or is compromised, get a new card, account number, and password. Do not use your old password. When creating a password, don't use common numbers like the last four digits of your social security number or your birth date.

6. Fraudulent change of address. Notify the local Postal Inspector if you suspect an identity thief has filed a change of address with the post office or has used the mail to commit credit or bank fraud. Find out where the fraudulent credit cards were sent. Notify the local Postmaster for the address to forward all mail in your name to your own address. You may also need to talk to the mail carrier.

7. Social Security number misuse. Call the Social Security Administration to report fraudulent use of your social security number. As a last resort, you might want to change the number. The SSA will only change it if you fit their fraud victim criteria. Also order a copy of your Earnings and Benefits Statement and check it for accuracy.

8. Passports. If you have a passport, notify the passport office in writing to be on the lookout for anyone ordering a new passport fraudulently.

9. Phone Service. If your long distance calling card has been stolen or you discover fraudulent charges on your bill, cancel the account and open a new one. Provide a password which must be used anytime the account is changed.

10. Driver License number misuse. You may need to change your drivers license number if someone is using yours as identification on bad checks. Call the state office of the Department of Motor Vehicles (DMV) to see if another license was issued in your name. Put a fraud alert on your license. Go to your local DMV to request a new number. Also, fill out the DMV's complaint form to begin the fraud investigation process. Send supporting documents with the complaint form to the nearest DMV investigation office.

11. False civil and criminal judgements. Sometimes victims of identity theft are wrongfully accused of crimes committed by the imposter. If a civil judgement has been entered in your name for actions taken by your imposter, contact the court where the judgement was entered and report that you are a victim of identity theft. If you are wrongfully prosecuted for criminal charges, contact the state Department of Justice and the FBI. Ask how to clear your name.