WHAT TO DO IF YOU ARE A VICTIM OF IDENTITY THEFT

- Call the toll-free fraud number of any one of the three major credit bureaus and have a fraud alert placed on your credit report. This can help prevent an identity thief from opening additional accounts in your name. As soon as the credit bureau confirms your fraud alert, the other two credit bureaus will automatically be notified to place fraud alerts on your credit reports, and all three reports will be sent to you free of charge.

- Close any accounts that have been tampered with or opened fraudulently. If you close existing accounts and open new ones, use new personal identification numbers (PINs) and passwords. If there are fraudulent charges or debits, ask the company for the necessary forms to dispute the transactions. If your checks have been stolen or misused, close the account and ask your financial institution to notify the appropriate check verification service.

- File a report with your local police or the police in the community in which the identity theft took place. Keep a copy of the report in case it is needed to validate your claims to creditors.

- File a complaint with the Federal Trade Commission. By sharing your complaint, you will provide important information that can help law enforcement officials track down identity thieves and stop them. The FTC can also refer victim complaints to other appropriate agencies and companies for further action.

CONTACT INFORMATION

CREDIT BUREAUS:

Equifax — www.equifax.com
P.O. Box 740241, Atlanta, GA 30374-0241
To report fraud: 800-525-6285 / TDD 800-255-0056
To order a credit report: 800-685-1111

Experian — www.experian.com
P.O. Box 9532, Allen, TX 75013
To report fraud: 888-397-3742 / TDD 800-972-0322
To order a credit report: 888-397-3742

TransUnion — www.transunion.com
P.O. Box 6790, Fullerton, CA 92634-6790
To report fraud: 800-680-7289 / TDD 877-553-7803
Fax: 714-447-6034; e-mail: fvad@transunion.com
To order a credit report: 800-888-4213

To "opt out" of receiving pre-screened credit card offers: 888-567-8688

FEDERAL TRADE COMMISSION:

To file a complaint, visit www.consumer.gov/idtheft or call the FTC's toll-free Identity Theft hotline @ 877-438-4338 / TDD 202-326-2502 or write to:
Identity Theft Clearinghouse
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

SOCIAL SECURITY ADMINISTRATION:

To report fraud: 800-269-0271 / fax: 410-597-0118
E-mail: oig.hotline@ssa.gov
SSA Fraud Hotline
P.O. Box 17768
Baltimore, MD 21235

NATIONAL DO NOT CALL REGISTRY:

888-382-1222 or www.donotcall.gov

DIRECT MARKETING ASSOCIATION:

To "opt out" of receiving direct mail marketing:
Mail Preference Service
P.O. Box 643
Carmel, NY 10512
To "opt out" of receiving unsolicited commercial e-mails: www.dmaconsumers.org/offemaillist.html

IDENTITY THEFT

Bloomington Police Department
305 S. East Street
Bloomington, Illinois 61701

Public Affairs Unit
(309) 434-2355
(309) 434-2534
police@cityblm.org

DEFINING IDENTITY THEFT

Identity theft is the unauthorized use of another person's personal identifying information (name, address, date of birth, Social Security number, mother's maiden name, etc.) to commit financial fraud.

HOW IDENTITY THIEVES GET YOUR PERSONAL INFORMATION

- By stealing wallets and purses containing ID, credit and bank cards
- By stealing mail, including bank and credit card statements, pre-approved credit offers, new checks, and tax information
- By completing "change of address" forms to divert your mail to another location
- By rummaging through your trash for personal data — a practice known as "dumpster diving"
- By fraudulently obtaining your credit report by posing as a landlord, employer, or someone with a legitimate right to such information
- By using personal information you share on the Internet
- By scamming you, often through e-mail, posing as legitimate companies or government agencies with which you do business
- Through "business record theft" — stealing files from offices where you are a customer, employee, patient or student… bribing an employee who has access to your files… or hacking into electronic files
- By taking personal information from your home

HOW IDENTITY THIEVES USE YOUR PERSONAL INFORMATION

- By calling your credit card issuer and, pretending to be you, asking to change the mailing address on your account. Because your bills are being sent to the new address, it may take some time before you realize there are fraudulent charges on your account

(continued from previous page)

- By opening a new credit card account, using your name, date of birth and Social Security number. When the bill goes unpaid, the delinquency is put on YOUR credit report
- By opening a bank account in your name and writing bad checks on that account
- By establishing phone or wireless service in your name
- By filing for bankruptcy under your name to avoid paying debts they've incurred under your name, or to avoid eviction from their residence
- By counterfeiting checks or debit cards, and draining your bank account
- By making expensive purchases, such as cars and high-priced electronics, in your name
- By giving your name to the police during an arrest. When they fail to show up for a court date, an arrest warrant is issued in your name

TYPES OF INFORMATION TO GUARD FROM IDENTITY THIEVES

- Social Security number
- Driver's license number / State ID cards
- Mother's maiden name
- Current and past addresses
- Credit and Debit card numbers
- Personal ID numbers, access codes, and passwords
- Passports
- Firearm owner ID cards
- Employee ID cards
- Birth certificates
- Telephone numbers
- Birth date

GUARDING AGAINST IDENTITY THEFT

- Order a copy of your credit report from each of the three major credit bureaus once a year. Check the contents carefully and make sure the information is correct and includes only those activities you have authorized.
- Put passwords on your credit card, bank and phone accounts. Avoid using easily available information such as your birth date, the last four digits of your Social Security number or a series of consecutive numbers. When opening new accounts, use a password instead of your mother's maiden name if the application asks for that.
- Ask about information security procedures in your workplace. Verify that records are kept in secure locations and find out who has access to your personal information.
- Secure personal information in your home if you have roommates, employ outside help such as cleaning companies, and when you are having service work done in your home.
- Don't give out personal information such as account numbers over the phone, through the mail or over the Internet, unless you initiated the contact.
- Limit the amount of personal information that is printed on your checks.
- Shred personal documents such as payment receipts and pre-approved credit offers before putting them in the trash.
- Don't put outgoing mail in your mailbox. Take it to the Post Office instead.
- Stop mail and newspaper delivery when you are planning to be away from home for extended periods.
- Contact creditors if you suspect bills, especially credit card statements, have not arrived on time.
- Give out your Social Security number only when absolutely necessary. You don't have to give the number to a business just because they request it.
- Update your computer anti-virus software regularly. Use encryption when possible.