Identity Fraud

What is Identity Fraud?

The practice of identity fraud has plagued victims for decades. In the past, thieves stole wallets, ravaged dumpsters and accessed mass marketing lists for victims' personal identifying information. The advent of the Internet in the 1990s provided thieves with greater anonymity and opportunity to steal and sell victims' identifying information. Incidents of identity fraud soared as a result.

Perpetrators steal victims' identifying information and sell it or use it illegally for their own benefit. Identifying information might include a victim's name, address, telephone number, driver's license number, social security number, place of employment, employee identification number, mother's maiden name, bank account number, credit card number or computer password identification, or even digital fingerprint images.

Thieves might use the stolen information to open fraudulent credit card accounts, cell phone accounts, long distance telephone service, utility accounts, or to commit endless other types of fraud. They might also use another person's stolen identity to avoid criminal prosecution for crimes.

A single victim of identity fraud might be victimized in dozens of ways. Often, unsuspecting victims learn of the crime with a telephone phone call or letter from a creditor or collection agency warning victims about charges they know nothing about.

Most victims learn about the fraud after much damage has already been done. It can take months to determine the extent of the damage, and longer to correct a damaged credit history.

Identity fraud victims spend countless hours defending themselves against creditors and proving they did not purchase the disputed goods themselves.

All too often, victims are treated as though they are the criminals.

Identity Fraud and the Law

Recent years saw a flurry of legislative activity as legislators struggled to respond to the growing problem of identity fraud. Massachusetts enacted **ß 266-37E, Identity fraud and false impersonation**. Violation of the state law is a misdemeanor punishable by up to two-and-one-half years' incarceration. The law states that in addition to any other punishment, a person found guilty shall be ordered to make restitution for financial loss sustained by a victim as a result of the crime. The law defines financial loss to include any costs incurred by a victim in correcting a damaged credit history or any costs incurred because of civil or administrative proceedings related to debts arising from the crime, including lost wages and attorney fees.

The Commonwealth's law is unique in that it also prohibits use of stolen identifying information to commit harassment. The law might be applied in instances where a stalker or other individual poses as a victim to interfere with that victim's utilities or other services (e.g. having a victim's electricity turned off or subscribing to dozens of magazines in a person's name).

Reporting Identity Fraud

Because identity fraud laws are relatively new, and because of the many forms identity fraud takes, there is sometimes confusion about which law enforcement agency has jurisdiction over a particular incident. Identity fraud that happens in an unknown location or in cyberspace adds additional confusion to the question of jurisdiction.

Victims, law enforcement professionals, prosecutors and victim service providers face complicated challenges in responding to identity fraud. Because of some individuals' confusion or unfamiliarity with the new laws, and because of the complex nature of identity fraud, victims might find themselves frustrated by a lack of response on the part of the criminal justice system.

The following information includes suggested steps identity fraud victims can take to protect themselves and agencies that can help victims find the assistance they need.

For Victims: What Should You Do?

Experts recommend a number of steps you should take immediately to protect yourself and prevent further damage.

Keep a record, in one place, of every action you take related to the fraud. Include every telephone call that you make, the name of every person you speak to, and copies of every letter you send or form you fill out related to the fraud.

1. Contact the three major credit bureaus, Experian (formerly TRW), Trans Union and Equifax, and inform them that you believe you are a victim of fraud. Their contact information appears at the end of this document. Contact the agencies both by telephone and in writing. They will place a ìfraud alertî on your account. Any creditor who receives an application for credit in your name will learn about the fraud alert when they call to check your credit history. In addition, the credit bureaus will not give out information about your credit history without your permission for as long as the fraud alert is in place.

By law, the credit bureaus must provide fraud victims with one free copy of your credit report. The three credit bureaus will each send you a copy of your report once you notify them that you are a fraud victim. Check each report over carefully for fraudulent accounts.

*Request another report six months later to check for new fraudulent accounts or damage to your credit history.

2. File reports about the fraud with your local police department, with the Federal Trade Commission (contact information follows). You can also contact your local office of the FBI or Secret Service to report identity fraud. If you believe the perpetrator used the U.S. Postal System to commit fraud, contact your local Postal Inspector.

3. Contact the Social Security Administration if you suspect that your Social Security number has been used to commit fraud, 1-800-269-0271.

4. Contact any bank or financial institutions where a perpetrator may have tampered with your accounts or where you believe a perpetrator has created new accounts in your name. Contact the Privacy Rights Clearinghouse, listed below, for information about working with check verification companies to deal with any fraud involving banks or financial institutions.

5. Contact any other agency or creditor with whom your name or identifying data may have been fraudulently used.

Resources for Identity Fraud Victims

For reporting fraud:

• Credit reporting bureaus:

Equifax
P.O. Box 740250
Atlanta, GA 30374-0250
(800) 525-6285

Experian (formerly TRW)
P.O. Box 1017
Allen, TX 75013
(888) EXPERIAN
www.experian.com

Union
P.O. Box 390
Springfield, PA 19064
(800) 680-7289
www.tuc.comTrans

• Federal Trade Commission (FTC)
Consumer Response Center
600 Pennsylvania Avenue, N.W.
Washington, DC 20580
(877) ID THEFT (877-438-4338)
TDD (202) 326-2502

For information, support, advocacy and referrals:

Massachusetts Office for Victim Assistance
One Ashburton Place, Suite 1101
Boston, MA 02108
(617) 727-5200

Privacy Rights Clearinghouse
1717 Kettner Ave., Ste. 105
San Diego, CA 92101
(619) 298-3396
www.privacyrights.org

National Center for Victims of Crime
2111 Wilson Blvd., Ste. 300
Arlington, VA 22201
1-703-276-2880
Information and referral line:
1-800-FYI-CALL
www.ncvc.org