Tel: 508/832-7777
Fax: 508/832-7781

AUBURN POLICE DEPARTMENT

416 Oxford Street, North • Auburn, Massachusetts 01501

Andrew J. Sluckis Jr., *Chief of Police*

Identity Theft / Fraud Victim Assistance Kit

This packet will provide victims with a list of resources and instructions when dealing with an identity theft situation. The Auburn Police Department will assist victims associated with this crime, but unfortunately, the victims themselves are burdened with resolving their own credit problems. Victims of identity theft must act quickly and assertively to minimize the damage to their good name. When dealing with the authorities and financial institutions, try to keep a log of all your conversations, including dates, times, names, and phone numbers. In this packet, there will be a worksheet for your convenience when logging this contact information.

In this assistance kit, you will find an ID theft affidavit supplied by the FTC (Federal Trade Commission). This affidavit has been adapted by all financial and credit institutions when filing fraudulent activities to personal accounts. If you find that you're a victim of identity theft, the Auburn Police Department immediately urges you to take the following steps:

In Memory of Patrolman
Stephen A. Lukas
1960 - 1986

Place a security freeze on your credit report

Effective October 2007, Massachusetts consumers can place a security freeze on their credit report, prohibiting a credit reporting agency from releasing any information from the report without written authorization (M.G.L. c. 93, § 56 and M.G.L. c. 93, § 62A).

If you have been a victim of identity theft, and you provide the credit reporting agency with a valid police report, it cannot charge you to place, lift or remove a security freeze. In all other cases, a credit reporting agency may charge up to $5 each to place, lift or remove a security freeze.

Victims of identity theft must send a written request to each of the credit bureaus (Equifax, Experian, and TransUnion) by regular, certified or overnight mail and include name, address, date of birth, social security number, and credit card number and expiration date for payment, if applicable. Each credit bureau has specific requirements to place a security freeze.

The credit bureaus have three business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze.

Contact credit bureaus and place a fraud alert on your credit file

Contact the fraud department of any one of the three major credit bureaus to place a fraud alert on your credit file. The fraud alert requires that creditors contact you before opening any new accounts or making any changes to your existing accounts. When you place a fraud alert on your credit file, all three credit bureaus are required by law to automatically send a credit report free of charge to you.

This "one-call" fraud alert will remain in your credit file for at least 90 days. When you get your three credit reports, review them carefully. Look to see whether there are any accounts that you did not open, unexplained debts on your true accounts, and inquiries that you didn't initiate. Contact any companies if there is any unexplained activity:

Equifax
P.O. Box 740241
Atlanta, GA 30374-0241
1-800-685-1111
Report fraud: 1-800-525-6285
TDD: 800-255-0056
www.equifax.com

TransUnion
P.O. Box 6790
Fullerton, CA 92634-6790
Email: fvad@transunion.com
1-800-888-4213
Report fraud: 1-800-680-7289
TDD: 877-553-7803
www.transunion.com

Experian
P.O. Box 9532
Allen, TX 75013
1-888-397-3742
Report fraud: 1-888-397-3742
TDD: 800-972-0322
www.experian.com

Contact the fraud departments of each of your creditors

Make phone calls today if your cards have been stolen. If your ATM or debit card has been stolen, even if you are unsure whether these cards have been used, report the thefts immediately to your bank or card issuer. If your credit cards have been stolen, also report these thefts immediately, whether or not you are aware that the cards have been used.

When obtaining new accounts from your creditors, make sure to use **new** personal identification numbers (PINs) and passwords. Make a list of all of the financial institutions where you do business, including your credit card companies and all of the financial institutions where you have checking, savings, investment, or other accounts.

You should also identify your telephone, cell phone and Internet Service Providers and report to each of these companies that you have been the victim of identity theft, even if that particular company has not been the subject of the fraud. Ask each of your creditors to place a "fraud alert" on your account.

Place an extended alert on your credit file. If you made an identity theft report to a police department, you may submit a copy of that report to any of the three major credit bureaus, and then an extended fraud alert will be placed in your credit file for a 7-year period.

Having a fraud alert on your credit file means that any time a "user" of your credit report (for instance, a credit card company, lender, or other financial institution) checks your credit report, it will be notified that you did not authorize any new credit cards, any increase in credit limits, the issuance of a new card on an existing account, or other increases in credit, unless the "user" takes extra precautions to ensure that it is giving the additional credit to you (and not to the identity thief).

Contact your banking institution

You may learn that the identity thief has written checks in your name. If so, you need to alert your bank and act immediately … **TIME MATTERS!!** If your checks have been stolen, or if you believe they have been used, contact your bank or credit union and stop payment right away.

Put stop payments on any outstanding checks that you are unsure about. If you suspect your accounts have been compromised, cancel your checking and savings accounts and obtain new account numbers.

Ask your bank to notify appropriate check verification services that you have been the victim of identity theft. Many retail stores use check verification systems, and you can alert check verification systems about the identity theft, and ask them to stop accepting checks in your name drawn on the account you are closing.

Promptly make a report with your local police department

File a police report with your local police department, keep a copy for yourself, and give a copy to your creditors and the credit bureaus. In the State of Massachusetts, identity theft is a crime but you should be aware that not all identity theft complaints can or will be investigated. However, by providing law enforcement officials with a written report, you make it possible for officers to spot trends and patterns, and to identify the prevalence of identity theft.

(M.G.L. c. 266, s. 37E) - A law enforcement officer shall accept a police incident report from a victim and shall provide a copy to such victim, if requested, within 24 hours. Such police incident reports may be filed in any county where a victim resides, or in any county where the owner or license holder of personal information stores or maintains said personal information, the owner's or license holder's principal place of business or any county in which the breach of security occurred, in whole or in part.

Registry of Motor Vehicles

If you were issued a driver's license by the Massachusetts Registry of Motor Vehicles, you may use the RMV's website for information about obtaining a new driver's license at www.mass.gov/rmv.

Social Security Administration

Contact the Social Security Administration to request a replacement card if your Social Security card was lost or stolen, or to request a new Social Security number in certain circumstances, or for help to correct your earnings records. You may also contact the Office of the Inspector General to report Social Security number misuse that involves buying or selling Social Security cards, or may involve people with links to terrorist groups or activities. Contact the Fraud Hotline at 1-800-269-0271.

United States Postal Service

Notify the U.S. Postal Inspection Service if you suspect that an identity thief has filed a change of your address with the post office. You will also need to notify your local postmaster to make sure that all mail in your name comes to your address.

Passport Services Office

If your passport was stolen, you should immediately report that your passport was stolen to the U.S. Department of State Passport Services Office. To obtain a new passport, you must also complete the "Application for Passport: DS-11" and submit it in person. For instructions and to download these forms, visit the website for the Passport Services Office at www.travel.state.gov/passport.