THE COMMONWEALTH OF MASSACHUSETTS
OFFICE OF THE ATTORNEY GENERAL
ONE ASHBURTON PLACE
BOSTON, MASSACHUSETTS 02108

MAURA HEALEY
ATTORNEY GENERAL

(617) 727-2200
(617) 727-4765 TTY
www.mass.gov/ago

Attorney General Maura Healey's Guide on Identity Theft for Victims and Consumers

Identity theft is a serious crime with serious costs for victims. ID theft occurs when someone obtains your personal information – such as your Social Security Number, credit card or account numbers, passwords, among others – to defraud or commit crimes. Victims of identity theft may lose significant money and time, and may find their reputation and credit rating has been damaged, affecting their ability to obtain loans for education or housing, approval for rental agreements, and approval for credit cards or large purchases requiring credit.

I. If You Are a Victim of Identity Theft, p. 1-4
II. Avoiding Identity Theft, p. 4-6
III. Resources, p. 7

I. If You Are a Victim of Identity Theft

Take actions immediately to minimize damage to your credit record, and to ensure that you are not held responsible for debts which the identity thief incurred using your name. Keep a record of all correspondence and conversations with financial institutions and other companies, credit bureaus, and law enforcement officials. Send all correspondence by certified mail, return receipt requested, to document what the company received and when. Keep copies of everything.

A. What Do I Do First? Take the following steps as soon as you discover you have been a victim of identity theft.

1.) 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. Massachusetts law provides that identity theft is a crime (M.G.L. c. 266, s. 37E). You should be aware that not all identity theft complaints can or will be investigated. However, by providing law enforcement offices with a written report, you make it possible for law enforcement offices to spot trends and patterns, and to identify the prevalence of identity theft.

2.) 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, 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. Review these requirements on the websites for each prior to sending your written request. Please see the **Resources** section of this publication (pages 6-8) for contact information for each credit bureau.

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.

3.) **Close any problem accounts.** Contact the credit card companies, banks, or any other creditors to close the accounts that you know have been tampered with or opened fraudulently.

4.) **Contact the 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. Please see the **Resources** section of this publication (pages 6-8) for contact information for each credit bureau.

5.) **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. If you are 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. To make sure that each of your creditors is aware that an identity thief may have your account information, 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. It is a good idea to follow up in writing to each of the companies that you contact, and to keep a record of your letters.

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 one 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 do 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).

B. Who Do I Need to Contact? After taking the steps above, review all credit, billing, and bank statements with great care after you have been the victim of identity theft, and report all questionable activities to the appropriate company or financial institution.

1.) Your Bank. You may learn that the identity thief has written checks in your name. If so, you need to alert your bank, and close your bank account. (Remember to discuss with your bank representative what to do about outstanding checks that have not yet been cashed.) 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. The major check verification companies are:

i. CheckRite (800) 766-2748
ii. ChexSystems (800) 428-9623 (closed checking accounts)
iii. CrossCheck (800) 552-1900
iv. Equifax (800) 437-5120
v. National Processing Co. (NPC) (800) 526-5380
vi. SCAN (800) 262-7771
vii. TeleCheck (800) 710-9898

2.) 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.

3.) 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. To report fraud, contact the Social Security Administration Office of the Inspector General Fraud Hotline at 1-800-269-0271. For additional contact information, please see the **Resources** section.

4.) 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. For additional contact information, please see the **Resources** section.

5.) **Passport Services Office.** If your passport was stolen, you should immediately report that your passport was stolen by completing a written form (called "Statement Regarding Lost or Stolen Passport: DS-64") provided by 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. For additional contact information, please see the **Resources** section.

6.) **Cellular or mobile provider.** If you discover fraudulent charges on your cell phone or mobile service bill, contact your provider immediately. You will probably need to close your accounts and open new ones. You may also want to request that a password be provided and required before any changes can be made to your accounts.

II. Avoiding Identity Theft

A. **Be Aware of How Thieves Obtain Personal Information.** Identity thieves can steal your personal information from a number of sources, such as bank statements, discarded credit card and ATM receipts, stolen mail, pre-approved credit card applications, and passports, among others. Thieves may obtain these items by searching through your trash, or stealing a wallet or purse that contains credit cards, social security card, or driver's license. Identity thieves may also obtain your personal information by way of the Internet or phone, including through unsecured Internet websites, fraudulent telemarketing calls, fraudulent emails and Internet websites, computer viruses and spyware, or even by using computer software found on public access computers or surreptitiously installed on home computers that log your keystrokes.

B. **Know Your Rights in the Event of a Security Breach.** Any entity (including individuals) that maintain or store personal information are now required by law (M.G.L. c. 93H) to notify the Attorney General's Office and the Office of Consumer Affairs and Business Regulations in the event of a data breach, in which access to that information is compromised. The notification must take place "as soon as practicable and without unreasonable delay," and must include the nature of the breach, the number of residents of the Commonwealth affected by the breach, and any steps the agency has taken or plans to take relating to the incident. These entities must also notify affected residents in the event of a data breach. The notification must include the consumer's right to obtain a police report and any instructions for requesting a security freeze on a credit report. Consumers also must be allowed access to additional information such as the date or approximate date of the data breach and any steps the agency has taken or plans to take relating to the incident.

   Notifications may be written, or distributed electronically. Notification to consumers may only be delayed if a law enforcement agency determines that notification will impede a criminal investigation.

C. **Manage Your Personal Information.** Do not routinely carry your social security card or birth certificate in your wallet or purse. Carry only those credit cards you use regularly and cancel all credit cards you do not use. Don't give out any personal information on the telephone, through the mail, or over the Internet, unless you've initiated the contact or are sure you know with

whom you are dealing. Disclose your social security number only when absolutely necessary. Social Security numbers were implemented as a method to account for your taxable earnings, not as a universal identifier. Change your driver's license number to a randomly assigned "S number." When you pay by check, the seller can only record your name, address, driver's license or Massachusetts ID number, and your choice of a home or daytime telephone number (M.G.L. c. 93, s. 105). If you have a random license number, you avoid disclosing your Social Security number every time you pay by check.

Keep an accurate list of all credit cards and bank accounts including the name, mailing address and telephone number of the creditor, the account number, and expiration date. Update the list regularly and keep it in a secure place. Also, review closely all credit card and bank statements each month to detect unusual activity or unauthorized charges. Deposit outgoing mail in post office collection boxes or at your local post office instead of an unsecured mailbox. Remove mail promptly from your mailbox. If you're planning to be away from home and can't pick up your mail, call the U.S. Postal Office at 1- 800-275-8777, to ask for a vacation hold. Destroy all credit card and ATM receipts and do not discard them at banks or retail establishments. Destroy pre-approved credit card solicitations and reduce the number of those solicitations by calling 1 (888) 5-OPT-OUT (1-888-567-8688), or visit the website at www.optoutprescreen.com.

Massachusetts law requires that any entity that maintains personal information comply with specific standards for disposal of that information: paper documents containing personal information must be either redacted, burned, pulverized or shredded so that personal data cannot practicably be read or reconstructed; and electronic media and other non-paper media containing personal information must be destroyed or erased so that personal information cannot practicably be read or reconstructed. Corporations, organizations and agencies may be fined for violating these standards.

D. Safeguard Your Computer. Update your virus protection software regularly. Computer viruses can have damaging effects, including introducing programs that cause your computer to send out files or other stored information. Update the security protections on your operating system by downloading any security updates or patches.

Don't download files from strangers or click on hyperlinks from people you don't know. Opening a file could expose your system to a computer virus or a program that could hijack your computer or modem. Use a firewall, especially if you have a high-speed or "always on" connection to the Internet. The firewall allows you to limit uninvited access to your computer. Use a secure browser. When you're submitting information on the Internet, look for the "lock" icon on the status bar. It's a symbol that your information is secure during transmission. Avoid using an automatic log-in feature that saves your username and password, and always log off when you're finished. Try not to store financial information on your laptop unless absolutely necessary. If you do, use a password that is a combination of letters, numbers, and symbols.

Don't respond to unsolicited emails that ask for personal information, even if it appears to come from a legitimate bank or other business. ID thieves will replicate emails and websites from legitimate companies, including banks and other financial institutions, to try to trick you into revealing your personal information. This tactic is called "phishing."

E. Monitor Your Credit Reports. A credit report contains information such as where you work and live, all the credit accounts that have been opened/closed in your name, and whether you pay your bills on time. Check to see if you have authorized everything on your credit report.Under state and federal law, you are entitled to one free copy of your credit report each year from each of the three credit reporting agencies. You are also entitled to a free credit report when you request that a fraud alert be placed in your credit file, as described above in this document. Exercise this right, and check your credit report closely for accuracy. You can order your credit report by calling each of the three credit reporting agencies directly (please see the "Resources" section of this publication), or you can order all three reports by contacting the centralized source: 1 (877) FACT-ACT (1-877-322-8228), or visit the website at www.annualcreditreport.com.

In general, if you request more than one credit report each year, and you have not placed a fraud alert in your credit file, credit reporting agencies may charge you no more than $8.00 for a copy of your credit report.

F. Individuals in the Military. If you are on active military duty, consider placing an alert on your credit file. An alert will appear on your credit file for a 12-month period and special care must be taken before extending credit in your name. It also means that for two years from the date you make a request to have an active military duty alert placed on your credit file, credit bureaus must exclude you from any lists of consumers they provide to any third party to offer credit or insurance to you when you did not initiate the transaction.

III. Resources

State and Federal Consumer Agencies

Office of Attorney General Maura Healey
One Ashburton Place
Boston, MA 02108
Phone: (617) 727-2200
TTY: (617) 727-4765
Consumer Hotline: (617) 727-8400
www.mass.gov/ago

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
Identity Theft Helpline: 1-877-ID-THEFT (1-877-438-4338)
TTY: 1-866-653-4261
www.consumer.gov/idtheft
www.ftc.gov

Massachusetts Office of Consumer Affairs and Business Regulation
Ten Park Plaza, Suite 5170
Boston, MA 02116
Phone: (617) 973-8700
Consumer Hotline: (617) 973-8787
(888) 283-3757
www.mass.gov/consumer

Credit Reporting

AnnualCreditReport.com
Central source for annual free credit reports from all credit reporting agencies
Order credit reports by phone: 1-877-322-8228
Opt out of pre-approved offers: 1 (888) 5-OPT-OUT (1-888-567-8688)
www.annualcreditreport.com

Equifax
Order credit reports by phone: 1-800-685-1111
Place a fraud alert on a credit: 1-888-766-0008
www.equifax.com

Experian
Order credit reports by phone: 1-888-397-3742
To report fraud or identity theft: 1-888-397-3742
www.experian.com

TransUnion
Order credit reports by phone: 1-877-322-8228
Dispute an item on your credit report: 1-800-916-8800
Fraud Victim Assistance Department: 1-800-680-7289
www.transunion.com

Other Helpful Resources

Massachusetts Registry of Motor Vehicles
Phone: (617) 351-4500
Toll-free: 1-800-858-3926
TTY: 1-877-768-8833
www.mass.gov/rmv

U.S. Postal Service
Phone: 1-800-ASK-USPS (1-800-275-8777)
TTY: 1-877-TTY-2HLP (1-877-889-2457)
www.usps.com

U.S. Department of State Passport Services Office
Phone: 1-877-487-2778
www.travel.state.gov/passport

Social Security Administration
Office of the Inspector General
Fraud Hotline: 1-800-269-0271
TTY: 1-866-501-2101
www.ssa.gov
www.ssa.gov/oig