Dalton Police Department

Identity Theft

* Information and guidelines for victims

Identity theft is an unlawful use of another person's personal information, such as name and date of bath, credit card numbers, Social Security number, or driver's license information for committing fraud or some other for deception. It is one of the fastest growing forms of criminal conduct in the United States. The Federal Trade Commission has estimated that 43% of fraud committed in the United States in 2002 was related to identity theft. Although the unauthorized use of another person's identity is in itself a crime under federal and Massachusetts law, it is almost always a means of committing other crimes such as bank fraud, check fraud, credit card fraud, Internet fraud, the fraudulent obtaining of loans, or the avoidance of criminal prosecution.

The first step in the compromising of a person's identity may be the theft of trash, the skimming of a credit card, the obtaining of information via the Internet, or some other technique that may not even be detected by the victim. In other cases, the theft of an identity may begin with the theft of a wallet or purse, or the interception of mail. Early detection of identity theft can minimize the amount of financial loss and the extent of damage done to your credit.

What should you do?

* Contact one of the following credit bureaus:

1. Equifax Credit Information Services
   1- 800 – 525 – 6285
   P.O. Box 740241
   Atlanta, GA 30374-0241
   www.equifax.com

2. Experian Information Solutions
   1 – 888 – 397 – 3742
   P.O. Box 9530
   Allen, TX 75013
   www.experian.com

3. Trans Union
   1 – 800 – 680 – 7289
   P.O. Box 6790
   Fullerton, CA 92634-6790
   www.transunion.com

* The credit bureaus are required to share information with each other about identity theft.

* Contact the Federal Trade Commission www.consumer.gov/idtheft

* If your Social Security number is involved, contact the Social Security Administration 1 – 800 – 269 – 0271 www.ssa.gov/oig

* Notify each financial institution there you have an account

* Maintain a log detailing each instance where your identity has been compromised, and each contact made with a financial institution, credit bureau, or law enforcement agency.

Identify theft investigations are very detailed and take time. Be patient, but do not hesitate to contact the investigator with any questions, or for updates on the case.

Dalton Police Department
462 Main St
Dalton, MA 01226
413-684-0300 • 413-684-6108 FAX
Anthony J. Riello • Chief of Police

Reporting a Lost or Stolen Credit Card

Name: _____

Address: _____ Phone: _____

Date of Birth: _____ SSN: _____

I, _____, in good faith am reporting that the following credit card is lost or has been stolen:

1. Credit Card Name: _____
   Account number: _____
2. Credit Card Name: _____
   Account number: _____
3. Credit Card Name: _____
   Account number: _____
4. Credit Card Name: _____
   Account number: _____

I have reported the cards to me Credit Card Company and identified any fraudulent charges if any. I am now reporting the cards lost/stolen to the Dalton Police Department so I may obtain a police report to give to my credit card company as well to initiate a criminal investigation.

I understand that falsely reporting a credit card as lost or stolen to the police is a crime under Massachusetts General Law Chapter 266 section 37 B/D that states:

On _____, (date of offense), with the intent to defraud, did make a false statement in representing a credit card to be lost or stolen. Penalty: not more than a year in the jail or house of correction and not more than $500 fine; or both.

Signature: _____ Date: _____

Officer taking report: _____

Dalton Police Department
462 Main St
Dalton, MA 01226
413-684-0300 • 413-684-6108 FAX
Anthony J. Riello • Chief of Police

IDENTITY THEFT CHECKLIST

If you believe your personal information (social security number, date of birth, credit card, or bank account information) has been compromised and you are or may be the victim of identity theft, you MUST take the following necessary steps:

1. Contact one of the three national credit reporting agencies, Equifax (1-800-525-62585; www.equifax.com), Experian (1-800-397-3742; www.experian.com), or TransUnion (1-800-680-7289; www.transunion.com) to place a Fraud Alert (initial) on your credit files. That one agency will automatically notify the other two for you. You will received a copy of your credit reports and confirmation of the fraud alerts. A fraud alert will prevent any new accounts from being opened unless the creditor first verifies your identity,
    a. The fraud alert will remain on your credit report for 1 year, after which it will be removed. However, you can request an extended Fraud Alert for seven (7) years if you submit your request in writing to each of the three credit reporting agencies after you have taken steps 2 and 3 below. You also have the oprtion to freeze your credit reports. Visit the Massachusetts Attorney's Generals website at www.ago.state.ma.us for more detailed information.
2. File a report with your local police department and request a copy of the report for your file.
3. Complete a FTC (Federal Trade Commission) Identity Theft Affidavit, and have it notarized. Keep your original and send a copy, along with a copy of the police report, to each of the creditors with whom you are disputing a fraudulent account. You may also want to file a complaint with the FTC at 1-877-438-4338, www.ftc.gov, to help them track thieves and refer cases to law enforcement agencies.
4. Close the accounts that have been compromised or opened fraudulently as soon as possible. For additional security reason, consider placing passwords and/or closing all other accounts.
5. Notify the Social Security Administration Fraud Hotline, 1-800-269-0271, to alert them of your situation and request that your file be documented for "Fraud Alert". You also may want to review your annual Personal Earnings and Benefits Statement carefully for any discrepancies.
6. Remain vigilant indefinitely . . . the thief(s) may target you again.

It is import that you maintain good recording keeping (a file folder/binder and a journal) of all the steps you have taken. Document each phone call you make: write down the date, and the name of the person you spoke with. You may want to follow-up in writing after each conversation (send letter Certified Mail/Return Receipt Requested). Remember to keep a copy of all letters you write.

NOTEWORTHY:

- Because your file folder/binder contains confidential and personal information, remember to store it in a safe and secure location.
- If you change your address, email address or telephone number, be sure to notify your creditors and any credit monitoring company.

Form **14039** (December 2020)	Department of the Treasury - Internal Revenue Service **Identity Theft Affidavit**	OMB Number 1545-2139

Complete this form if you need the IRS to mark an account to identify questionable activity.

Section A - Check the following boxes in this section that apply to the specific situation you are reporting *(Required for all filers)*

☒ 1. I am submitting this Form 14039 for myself

☐ 2. This Form 14039 is submitted in response to a 'Notice' or 'Letter' received from the IRS
- Please provide 'Notice' or 'Letter' number(s) on the **line to the right** _____
- Please check box 1 in **Section B** and see special mailing and faxing instructions on reverse side of this form.

☐ 3. I am submitting this Form 14039 on behalf of my 'dependent child or dependent relative'
- Please complete **Section E** on reverse side of this form.

☐ 4. I am submitting this Form 14039 on behalf of another person *(other than my dependent child or dependent relative)*
- Please complete **Section E** on reverse side of this form.

Section B – Reason For Filing This Form *(Required)*

Check only **ONE** of the following boxes that apply to the person listed in **Section C** below. If the taxpayer in 'Section C' has previously submitted a Form 14039 to the IRS on the same affected tax year(s), there's no need to submit another Form 14039.

☐ **1. Someone used my information to file taxes, including being incorrectly claimed as a dependent**

☒ **2. I don't know if someone used my information to file taxes, but I'm a victim of identity theft**

Please provide an explanation of the identity theft issue, how you became aware of it and provide relevant dates.
If needed, please attach additional information and/or pages to this form.

Section C – Name and Contact Information of Identity Theft Victim *(Required)*

Victim's last name	First name	Middle initial	**Taxpayer Identification Number** *(Please provide 9-digit Social Security Number)*

Current mailing address *(apartment or suite number and street, or P.O. Box)* If deceased, please provide last known address

Current city	State	ZIP code

Tax Year(s) you experienced identity theft *(If not known, enter 'Unknown' in one box below)*	**What is the last year you filed a return**

Address used on last filed tax return *(If different than 'Current')*	**Names used on last filed tax return** *(If different than 'Current')*

City *(on last tax return filed)*	State	ZIP code

Telephone number with area code *(Optional) If deceased, please indicate 'Deceased'*	Best time(s) to call
Home telephone number Cell phone number	

Language in which you would like to be contacted ☐ English ☐ Spanish

Section D – Penalty of Perjury Statement and Signature *(Required)*

Under penalty of perjury, I declare that, to the best of my knowledge and belief, the information entered on this Form 14039 is true, correct, complete, and made in good faith.

Signature of taxpayer, or representative, conservator, parent or guardian	Date signed

Submit this completed form to either the mailing address or the FAX number provided on the reverse side of this form.

Average time to complete: 10 minutes

Identity Theft Victim's Complaint and Affidavit

A voluntary form for filing a report with law enforcement, and disputes with credit reporting agencies and creditors about identity theft-related problems. Visit identitytheft.gov to use a secure online version that you can print for your records.

Before completing this form:

1. Place a fraud alert on your credit reports, and review the reports for signs of fraud.
2. Close the accounts that you know, or believe, have been tampered with or opened fraudulently.

About You *(the victim)*

Now

(1) My full legal name: _____
First Middle Last Suffix

(2) My date of birth: _____
mm/dd/yyyy

(3) My Social Security number: _____-_____-_____

(4) My driver's license: _____ _____
State Number

(5) My current street address:

_____
Number & Street Name Apartment, Suite, etc.

_____
City State Zip Code Country

(6) I have lived at this address since _____
mm/yyyy

(7) My daytime phone: (____)_____
My evening phone: (____)_____
My email: _____

Leave (3) blank until you provide this form to someone with a legitimate business need, like when you are filing your report at the police station or sending the form to a credit reporting agency to correct your credit report.

At the Time of the Fraud

(8) My full legal name was: _____
First Middle Last Suffix

(9) My address was: _____
Number & Street Name Apartment, Suite, etc.

_____
City State Zip Code Country

(10) My daytime phone: (____)_____ My evening phone: (____)_____
My email: _____

Skip (8) - (10) if your information has not changed since the fraud.

The Paperwork Reduction Act requires the FTC to display a valid control number (in this case, OMB control #3084-0047) before we can collect – or sponsor the collection of – your information, or require you to provide it.

About You *(the victim) (Continued)*

Declarations

(11) I ☐ did OR ☐ did not authorize anyone to use my name or personal information to obtain money, credit, loans, goods, or services — or for any other purpose — as described in this report.

(12) I ☐ did OR ☐ did not receive any money, goods, services, or other benefit as a result of the events described in this report.

(13) I ☐ am OR ☐ am not willing to work with law enforcement if charges are brought against the person(s) who committed the fraud.

About the Fraud

(14) I believe the following person used my information or identification documents to open new accounts, use my existing accounts, or commit other fraud.

(14): Enter what you know about anyone you believe was involved (even if you don't have complete information).

Name: _____
First Middle Last Suffix

Address: _____
Number & Street Name Apartment, Suite, etc.

_____
City State Zip Code Country

Phone Numbers: (___)_____ (___)_____

Additional information about this person: _____

(15) Additional information about the crime (for example, how the identity thief gained access to your information or which documents or information were used):

(14) and (15): Attach additional sheets as needed.

_____
_____
_____
_____
_____
_____
_____

Documentation

(16) I can verify my identity with these documents:

(16): Reminder: Attach copies of your identity documents when sending this form to creditors and credit reporting agencies.

☐ A valid government-issued photo identification card (for example, my driver's license, state-issued ID card, or my passport).
If you are under 16 and don't have a photo-ID, a copy of your birth certificate or a copy of your official school record showing your enrollment and legal address is acceptable.

☐ Proof of residency during the time the disputed charges occurred, the loan was made, or the other event took place (for example, a copy of a rental/lease agreement in my name, a utility bill, or an insurance bill).

About the Information or Accounts

(17) The following personal information (like my name, address, Social Security number, or date of birth) in my credit report is inaccurate as a result of this identity theft:

(A) _____
(B) _____
(C) _____

(18) Credit inquiries from these companies appear on my credit report as a result of this identity theft:

Company Name: _____
Company Name: _____
Company Name: _____

(19) Below are details about the different frauds committed using my personal information.

____
Name of Institution | Contact Person | Phone | Extension

____
Account Number | Routing Number | Affected Check Number(s)

Account Type: ☐ Credit ☐ Bank ☐ Phone/Utilities ☐ Loan
☐ Government Benefits ☐ Internet or Email ☐ Other

Select ONE:
- ☐ This account was opened fraudulently.
- ☐ This was an existing account that someone tampered with.

____
Date Opened or Misused (mm/yyyy) | Date Discovered (mm/yyyy) | Total Amount Obtained ($)

____
Name of Institution | Contact Person | Phone | Extension

____
Account Number | Routing Number | Affected Check Number(s)

Account Type: ☐ Credit ☐ Bank ☐ Phone/Utilities ☐ Loan
☐ Government Benefits ☐ Internet or Email ☐ Other

Select ONE:
- ☐ This account was opened fraudulently.
- ☐ This was an existing account that someone tampered with.

____
Date Opened or Misused (mm/yyyy) | Date Discovered (mm/yyyy) | Total Amount Obtained ($)

____
Name of Institution | Contact Person | Phone | Extension

____
Account Number | Routing Number | Affected Check Number(s)

Account Type: ☐ Credit ☐ Bank ☐ Phone/Utilities ☐ Loan
☐ Government Benefits ☐ Internet or Email ☐ Other

Select ONE:
- ☐ This account was opened fraudulently.
- ☐ This was an existing account that someone tampered with.

____
Date Opened or Misused (mm/yyyy) | Date Discovered (mm/yyyy) | Total Amount Obtained ($)

(19): If there were more than three frauds, copy this page blank, and attach as many additional copies as necessary.

Enter any applicable information that you have, even if it is incomplete or an estimate.

If the thief committed two types of fraud at one company, list the company twice, giving the information about the two frauds separately.

Contact Person: Someone you dealt with, whom an investigator can call about this fraud.

Account Number: The number of the credit or debit card, bank account, loan, or other account that was misused.

Dates: Indicate when the thief began to misuse your information and when you discovered the problem.

Amount Obtained: For instance, the total amount purchased with the card or withdrawn from the account.

Your Law Enforcement Report

(20) One way to get a credit reporting agency to quickly block identity theft-related information from appearing on your credit report is to submit a detailed law enforcement report ("Identity Theft Report"). You can obtain an Identity Theft Report by taking this form to your local law enforcement office, along with your supporting documentation. Ask an officer to witness your signature and complete the rest of the information in this section. It's important to get your report number, whether or not you are able to file in person or get a copy of the official law enforcement report. Attach a copy of any confirmation letter or official law enforcement report you receive when sending this form to credit reporting agencies.

Select ONE:

- ☐ I have not filed a law enforcement report.
- ☐ I was unable to file any law enforcement report.
- ☐ I filed an automated report with the law enforcement agency listed below.
- ☐ I filed my report in person with the law enforcement officer and agency listed below.

(20):
Check "I have not..." if you have not yet filed a report with law enforcement or you have chosen not to. Check "I was unable..." if you tried to file a report but law enforcement refused to take it.

Automated report:
A law enforcement report filed through an automated system, for example, by telephone, mail, or the Internet, instead of a face-to-face interview with a law enforcement officer.

_____
Law Enforcement Department State

_____ _____
Report Number Filing Date (mm/dd/yyyy)

_____
Officer's Name (please print) Officer's Signature

_____ (____)_____
Badge Number Phone Number

Did the victim receive a copy of the report from the law enforcement officer? ☐ Yes OR ☐ No

Victim's FTC complaint number (if available): _____

Signature

As applicable, sign and date *IN THE PRESENCE OF* a law enforcement officer, a notary, or a witness.

(21) I certify that, to the best of my knowledge and belief, all of the information on and attached to this complaint is true, correct, and complete and made in good faith. I understand that this complaint or the information it contains may be made available to federal, state, and/or local law enforcement agencies for such action within their jurisdiction as they deem appropriate. I understand that knowingly making any false or fraudulent statement or representation to the government may violate federal, state, or local criminal statutes, and may result in a fine, imprisonment, or both.

_____ _____

Signature Date Signed (mm/dd/yyyy)

Your Affidavit

(22) If you do not choose to file a report with law enforcement, you may use this form as an Identity Theft Affidavit to prove to each of the companies where the thief misused your information that you are not responsible for the fraud. While many companies accept this affidavit, others require that you submit different forms. Check with each company to see if it accepts this form. You should also check to see if it requires notarization. If so, sign in the presence of a notary. If it does not, please have one witness (non-relative) sign that you completed and signed this Affidavit. If someone has used your Social Security number (SSN) to get a tax refund or a job, or you suspect your SSN has been stolen, alert the IRS using Form 14039 at **www.irs.gov/pub/irs-pdf/f14039.pdf**.

_____

Notary

Witness:

_____ _____

Signature Printed Name

_____ _____

Date Telephone Number

CHARLES D. BAKER
GOVERNOR

KARYN E. POLITO
LIEUTENANT GOVERNOR

COMMONWEALTH OF MASSACHUSETTS
Office of Consumer Affairs and Business Regulation
501 Boylston Street, Suite 5100, Boston, MA 02116
(617) 973-8787 FAX (617) 973-8799
www.mass.gov/consumer

MIKE KENNEALY
SECRETARY OF HOUSING AND ECONOMIC DEVELOPMENT

EDWARD A. PALLESCHI
UNDERSECRETARY

A Consumer's Checklist for Handling Identity Theft

Identity theft occurs when someone steals your personal information, such as your Social Security number or bank account information, to commit fraud or other crimes. Identity theft can take many forms and can leave your finances in disarray, or damage your credit rating. Below are some helpful reminders and resources to minimize the damaging effects of having your identity stolen.

If you are a victim of identity theft or believe you may be a victim, be sure to do each of the following:

- ☐ Consider placing a fraud alert on your credit file
  - ➢ Place a fraud alert on your credit file by contacting the fraud department of any of the three major credit reporting agencies.
    - i. A fraud alert requires creditors to contact you prior to opening a new account or making changes to an existing account. The fraud alert remains in place for at least 90 days.
    - ii. The fraud alert requires all three credit reporting agencies to send you a credit report for free.
- ☐ Obtain a copy of your credit report
  - ➢ You are entitled to one free credit report per year from each of the three major credit reporting agencies (Equifax, Experian, and TransUnion), but consumers who are victims of identity theft or suspect they could be should obtain one immediately and consider frequent monitoring of their reports.
  - ➢ You can request credit reports from the three major credit reporting agencies by calling (877) 322-8228 or visiting www.annualcreditreport.com
- ☐ Dispute unauthorized transactions
  - ➢ Write a letter to each credit reporting agency disputing any fraudulently opened accounts or information.
  - ➢ The credit reporting agency has 30 days to investigate and remove any erroneous or unverified information.

- ☐ Report the incident
  - ➢ Identity theft is a crime. File a police report with your local police department. Keep a copy for yourself and provide additional copies to each of your creditors and credit reporting agencies.
  - ➢ Note that some creditors rely on a credit score or another automated credit application system and may not see these alerts if they do not obtain your full consumer report.
  - ➢ Active military members
    i. If you are currently serving in our armed forces, you may wish to voluntarily place an active duty alert on your credit file. It serves as an extra protection, as additional steps must be taken to extend credit in your name.
    ii. For one year after the alert has been requested, credit reporting agencies exclude you from any lists they provide to third party insurance providers or creditors unless you consent to it.
- ☐ Consider placing a security freeze on your credit report
  - ➢ By placing a security freeze on a credit report, you can prohibit a credit reporting agency from releasing information from your credit report without your written permission. If you filed a police report and provided the credit reporting agency with a copy, the agency cannot charge you for placing or removing a security freeze. If not, the agency can charge up to $5 for each action.
  - ➢ Each credit reporting agency has its own requirements when administering a security freeze. To request a security freeze on your credit report, you must contact each of the three national credit reporting agencies individually. Be sure to check that you meet each reporting agency's individual requirements for placing a security freeze.
  - ➢ A reporting agency has three days to place a security freeze on your credit report and five days to provide both confirmation and a personal identification number (PIN) or password to make changes to the status of your security freeze.
- ☐ File a complaint with/report the situation to the FTC and Attorney General's Office
  - ➢ If you believe this is a recurring scam and wish to report it, contact both agencies to do so.
- ☐ Close affected accounts
  - ➢ Close all accounts you know have been opened fraudulently or tampered with by reaching out to your credit card companies, financial institutions, or other possible creditors.

- ☐ Additional Tips
  - ➢ Write down the names of anyone with whom you spoke, what was said, and the date of the conversation
    i. Keep all original documentation, such as police reports and letters to and from creditors. Send copies of all documents when needed.

Report the theft to:

- ☐ All companies who handle your personal accounts
  - ➢ If there are unexplained or unwarranted charges on your credit card statement, cell phone bill, utility bill or other miscellaneous billing statement, immediately contact your provider(s). You should also request a change of password to prevent further tampering with your account, and, in certain cases you may even need to open a replacement account.
- ☐ Federal Bureau of Investigation (FBI)
  - ➢ The FBI may also investigate some financial crimes. Typically, the FBI focuses on fraud rings engaged in conspiracies to defraud financial institutions.
  - ➢ You can file a report on their Internet Crime Complaint Center
- ☐ Passport Services Office
  - ➢ If your passport is stolen, immediately report it as such by completing the **form** ("Statement Regarding Lost or Stolen Passport: DS-64") provided by the U.S. Department of State Passport Services Office.
- ☐ Social Security Administration
  - ➢ If your Social Security card has been stolen, contact the Social Security Administration to request a replacement card.
- ☐ United States Postal Service (USPS)
  - ➢ If you believe an identity thief has filed for a change of address under your name, contact the U.S. Postal Inspection Service.
  - ➢ Postal Inspectors may have jurisdiction over your case if the identity thief has used the mail to commit credit or bank fraud.
  - ➢ If you can determine where the fraudulent credit cards or checks were sent, contact the local Postmaster for that address and file a complaint and a police report. Be sure to request that change of address forms submitted on your behalf **not be** accepted.

Helpful Contacts

State and Federal Government Agencies

Massachusetts Office of Consumer Affairs and Business Regulation
501 Boylston Street, Suite 5100
Boston, MA 02116
Consumer Hotline: (617) 973-8787
(888) 283-3757
www.mass.gov/consumer

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

Federal Bureau of Investigation (Mass. Regional Office)
201 Maple Street
Chelsea, MA 02150
Phone: (857) 386-2000

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

Credit Reporting

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

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

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

TransUnion
Order credit reports by phone: (877) 322-8228
Dispute an item on your credit report:
(800) 888-4213
Fraud Victim Assistance Department:
(800) 680-7289
www.transunion.com

Other Helpful Resources

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

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

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

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

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

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

Identity Theft Information for Taxpayers

Identity theft places a burden on its victims and presents a challenge to many businesses, organizations and governments, including the IRS. The IRS combats this crime with an aggressive strategy of prevention, detection and victim assistance.

What is tax-related identity theft?

Tax-related identity theft occurs when someone uses your stolen Social Security number (SSN) to file a tax return claiming a fraudulent refund. If you become a victim, we are committed to resolving your case as quickly as possible.

You may be unaware that this has happened until you e-file your return and discover that a return already has been filed using your SSN. Or, the IRS may send you a letter saying it has identified a suspicious return using your SSN.

Know the warning signs

Be alert to possible tax-related identity theft if you are contacted by the IRS about:

- More than one tax return was filed for you,
- You owe additional tax, have a refund offset or have had collection actions taken against you for a year you did not file a tax return, or
- IRS records indicate you received wages or other income from an employer for whom you did not work.

Steps for victims of identity theft

If you are a victim of identity theft, the Federal Trade Commission recommends these steps:

- File a complaint with the FTC at identitytheft.gov.
- Contact one of the three major credit bureaus to place a 'fraud alert' on your credit records:
  - www.Equifax.com 1-800-525-6285
  - www.Experian.com 1-888-397-3742
  - www.TransUnion.com 1-800-680-7289
- Close any financial or credit accounts opened by identity thieves

If your SSN is compromised and you know or suspect you are a victim of tax-related identity theft, the IRS recommends these additional steps:

- Respond immediately to any IRS notice; call the number provided.
- Complete IRS Form 14039, *Identity Theft Affidavit*, if your e-file return rejects because of a duplicate filing under your SSN or you are instructed to do so. Use a fillable form at IRS.gov, print, then attach form to your paper return and mail according to instructions.
- Continue to pay your taxes and file your tax return, even if you must do so by paper.
- If you previously contacted the IRS and did not have a resolution, contact us for specialized assistance at 1-800-908-4490. We have teams available to assist.

More information is available at: IRS.gov/identitytheft or FTC's identitytheft.gov.

About data breaches and your taxes

Not all data breaches or computer hacks result in tax-related identity theft. It's important to know what type of personal information was stolen.

If you've been a victim of a data breach, keep in touch with the company to learn what it is doing to protect you and follow the "Steps for victims of identity theft." Data breach victims should submit a Form 14039, *Identity Theft Affidavit,* only if your Social Security number has been compromised and IRS has informed you that you may be a victim of tax-related identity theft or your e-file return was rejected as a duplicate.

How you can reduce your risk

Join efforts by the IRS, states and tax industry to protect your data. Taxes. Security. Together. We all have a role to play. Here's how you can help:

- Always use security software with firewall and anti-virus protections. Use strong passwords.
- Learn to recognize and avoid phishing emails, threatening calls and texts from thieves posing as legitimate organizations such as your bank, credit card companies and even the IRS.
- Do not click on links or download attachments from unknown or suspicious emails.
- Protect your personal information and that of any dependents. Don't routinely carry Social Security cards, and make sure your tax records are secure.

See Publication 4524, *Security Awareness for Taxpayers* to learn more.

NOTE: The IRS does not initiate contact with taxpayers by email to request personal or financial information. This includes any type of electronic communication, such as text messages and social media channels.

Publication 5027 (Rev. 5-2018) Catalog Number 67495R Department of the Treasury **Internal Revenue Service** www.irs.gov