

IDENTITY THEFT

POLICY & PROCEDURE NO. 2.16	ISSUE DATE: 07/01/14
	EFFECTIVE DATE: 07/01/14
MASSACHUSETTS POLICE ACCREDITATION STANDARDS REFERENCED: 42.2.8	REVISION DATE:

I. GENERAL CONSIDERATIONS AND GUIDELINES

Identity theft is the unlawful use of another person's personal information, such as name and date of birth, credit card numbers, Social Security number, or driver's license information, for the purpose of committing fraud or some other form of deception. It is one of the fastest growing forms of criminal conduct in the United States.

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 the victim's credit.

The term "victim" in this policy refers to the person whose identity has been compromised, yet financial institutions, retail merchants and mail order companies often suffer greater financial loss than the citizen whose information has been unlawfully used.

II. POLICY

It is the policy of this police department to investigate instances where a citizen's identity has been compromised for an unlawful purpose.

- A. In each case of reported identity crime, whether the victim resides in this community or a fraudulent transaction occurs here, a police officer will conduct an investigation and immediately file a report.
- B. Officers investigating instances of identity theft will provide victims with information that will assist them in repairing their credit and diminishing the amount of theft.
- C. The department will refer to other law enforcement agencies' information about fraudulent transactions occurring in their jurisdictions.
- D. The department will seek to educate the public about the issue of identity crime, including methods for preventing it.

III. DEFINITIONS

- A. *Personal Identifying Information*: Any name or number that may be used, alone or in conjunction with any other information, to assume the identity of an individual, including any name, address, telephone number, driver's license number, social security number, place of employment, employee identification number, mother's maiden name, demand deposit account number, savings account number, credit card number or computer password identification.
- B. *Victim*: Any person who has suffered financial loss or any entity that provided money, credit, goods, services or anything of value and has suffered financial loss as a direct result of the commission or attempted commission of a violation of this section.

IV. PROCEDURES

A. Initial Investigation and Reporting

- 1. JURISDICTION: The jurisdiction for an identity theft victim to file a police report is very broad. A victim may file a police report: ¹
 - a. In any county where the victim resides;
 - b. In any county where the victim's personal information is stored or maintained or the principal place of business of the entity that stores or maintains the data; or
 - c. In the county where the breach of security occurred in whole or in part.

2. IDENTITY THEFT AFFIDAVIT [42.2.8(B)]

- a. Officers should recommend that victims use the Federal Trade Commission Identity Theft Affidavit.
- b. The form's instructions contain valuable information to the victim and also provide for the capture of the information necessary to meet the requirements of an "Identity Theft Report" and for police to conduct a thorough investigation.
- c. The victim should be encouraged to complete the form, have it notarized, and return a copy of the form to the investigating officer.
- d. A completed copy should be obtained and filed with the police report or the investigator's file.

3. IDENTITY THEFT REPORTS [42.2.8(A)]

- a. Police reports and incident numbers are critical documents for victims of identity theft to resolve issues with creditors and credit reporting agencies.
- b. The report can be used to:
 - 1) Permanently lock fraudulent information that results from identity theft from appearing on the victim's credit report;
 - 2) Ensure these debts do not reappear on the credit reports;
 - 3) Prevent a company from continuing to collect debts that result from identity theft, or selling them to others for collection; and
 - 4) Allow a victim to place an extended fraud alert on his or her credit report.
- c. The report must contain details about the accounts and inaccurate information that resulted from the identity theft.
- d. A report will be filed prior to the end of the officer's shift, unless unusual circumstances cause it to be filed at a later date.
 - 1) The victim's copy of an Investigative Case Report Form will meet the time requirements for the purpose of reporting.
 - 2) The officer's report should also be submitted.
- e. A victim shall be provided a copy of the police report within twenty-four hours of its being requested.²
- f. Financial institutions often require victims to forward a police report, so the filing of the report should never be delayed more than one tour of duty.

B. Assisting the Victim [42.2.8(c)]**1. RESOURCES FOR VICTIMS**

- a. Police officers investigating an identity theft must not only attempt to identify the subject(s) responsible, but also assist the victim in minimizing the damage done.
- b. An officer investigating an identity theft shall provide the victim with appropriate brochures, documents, other resources to assist the victim in stopping further victimization and correcting damage caused by the crime. In addition to victim brochures, these resources include:
 - 1) Dispute Letter for New Accounts;
 - 2) Dispute Letter for Existing Accounts; and
 - 3) Identity Theft Affidavit (Federal Trade Commission)].

2. VICTIM CONTACT WITH CREDIT BUREAUS

- a. Victims should be advised to contact one of the three major credit bureaus and place a fraud alert on their credit reports. As soon as the credit bureau confirms the fraud alert, the other two credit bureaus will automatically be notified to place fraud alerts. Once a fraud alert is placed, victims are entitled to order one free copy of their credit report from each of the three nationwide consumer reporting companies.
- b. The three credit bureaus are:
 - Equifax Credit Information Services
(800) 525-6285
P.O. Box 740241
Atlanta, GA 30374-0241
www.equifax.com
 - Experian Information Solutions
(888) 397-3742
P.O. Box 9530
Allen, TX 75013
www.experian.com
 - TransUnion
(800) 680-7289
Fraud Victims Assistance Division

P.O. Box 6790
Fullerton, CA 92634-6790
www.transunion.com

3. NOTIFICATIONS TO FINANCIAL INSTITUTIONS: The officer should ensure that the victim notifies each financial institution where the victim has an account, so that those institutions can check the accounts for undetected fraud.
4. FEDERAL TRADE COMMISSION: The officer should advise the victim to contact the Federal Trade Commission and file a complaint. Complaints should be filed online at www.consumer.gov/idtheft.
5. COMPROMISE OF SOCIAL SECURITY NUMBERS: In cases where a victim's Social Security number has been compromised, the Social Security Administration should be notified at 800-269-0271, or at www.ssa.gov/oig.
6. DOCUMENTING CONTACTS: The officer should advise the victim to maintain a log detailing each instance where his/her identity has been compromised, and each contact [s]he makes with a financial institution, credit bureau, store, or law enforcement agency.
7. ID THEFT AFFIDAVIT: The victim should be provided a blank ID Theft Affidavit, and be asked to provide the police department with a copy once it has been completed. Completed affidavits should be filed with the case. [42.2.8(B)]
8. INFORMATION SHARING: The officer should inform the victim that information about the case will be shared with the Identity Theft and Financial Crimes Task Force, and with bank security investigators that may be assigned to the case by the victim's bank.

C. Follow-up Investigation

1. INITIAL FOLLOW-UP
 - a. Cases that require an in-depth investigation may be referred to the department's Detective Bureau for follow-up.
 - b. Upon receiving the referral, the Detective Supervisor shall screen and evaluate the case for additional investigative resources.
 - 1) Cases that show little possibility of being investigated to a successful conclusion shall be closed.
 - 2) Cases which may be continued further by patrol personnel shall be returned to the referring officer for further investigation.
 - 3) Cases identified for further investigation shall be assigned to an investigator.

- c. Detectives assigned to investigate should follow up on promising leads which may include:
 - 1) Determining the point of compromise;
 - 2) Interviewing or causing to be interviewed employees of financial institutions and stores;
 - 3) Securing and preserving images of the suspects;
 - 4) Tracing goods fraudulently purchased;
 - 5) Interacting with bank and credit card company fraud departments; and
 - 6) Investigating instances where the victim's identity was used to avoid criminal prosecution.
 - d. Investigations which lead to another jurisdiction shall be coordinated with the appropriate federal, state, or local law enforcement agency.
 - e. Detectives must keep victims apprised of all significant developments in the investigation, and shall contact them in all instances where it is learned that their identity has been further compromised or used.
2. REFERRALS FROM OTHER LAW ENFORCEMENT AGENCIES
[42.2.8(D)]
- a. Referrals of identity theft from outside agencies will normally be referred to the duty officer.
 - b. Upon receiving a referral, the duty officer shall coordinate investigative efforts with the referring agency. This may include:
 - 1) Following-up on all leads as requested by the referring agency;
 - 2) Documenting all fraudulent transactions;
 - 3) Securing all available evidence, including photographs, stolen property, and relevant documents;
 - 4) Informing the referring agency, officer or agent of all significant developments in the investigation; and
 - 5) Preparing a comprehensive report of the follow-up investigation, and providing a copy to the referring law enforcement agency or official.
3. DISSEMINATION OF SURVEILLANCE PHOTOGRAPHS
- a. Images of subjects conducting transactions related to identity theft may be shared with other agencies through:
 - 1) State and regional identity theft and counter crime taskforces;

- 2) New England State Police Network; and
 - 3) MassMostWanted.org web site.
- b. The detective should also view images received from these and other sources to determine if a subject has committed crimes in other jurisdictions or suspects are known to the detective.

D. Prevention and Education [42.2.8(e)]

1. The department will keep the public informed on the subject of identity fraud in general, and specifically about steps that the public can take to prevent becoming a victim.
2. BROCHURES: The department will make brochures relating to avoiding identity theft available to the public.
3. PUBLIC PRESENTATIONS: The department will maintain an education and prevention program available for presentation to civic groups by members of the department.
4. WEB SITE: The department web site will maintain links to sites that offer information about identity theft.
5. MEDIA: The department will utilize the media where appropriate to warn citizens about trends in identity crime.

¹ M.G.L. c. 266, §37E.

² M.G.L. c. 266, §37E.