



Town of Lexington

Police Department

Subject: Identity Theft	
Reference: 42.2.8	
Effective Date: January 1, 2012	Review Date: Annually
By Order of: Mark J. Corr, Chief of Police	

Policy & Procedure

42Q

The Municipal Police Institute, Inc. (MPI) is a private, nonprofit charitable affiliate of the Massachusetts Chiefs of Police Association. MPI provides training and model policies and procedures for police agencies. This policy is an edited version of MPI Policy 2.16 "Identity Theft."

GENERAL CONSIDERATIONS AND GUIDELINES

Identity theft is the unlawful use of another person's personal information, such as name, date of birth, credit card numbers, Social Security, or driver's license numbers, 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 state 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, goods or services and the avoidance of criminal prosecution.

Compromising a person's identity may result from picking through trash, skimming of a credit card, obtaining of information via the Internet, or some other technique that may not be detected by the victim. In other cases, the theft of an identity may begin when a wallet or purse is stolen, or mail intercepted. Early detection of identity theft can minimize financial loss and the extent of damage done to a victim's credit history.

The term "victim" in this policy refers to a person whose identity has been compromised, yet financial institutions, retail merchants and mail order companies often suffer significant financial losses as well.

42Q-Identity Theft

It is the policy of the Lexington Police Department to investigate and document instances where a person's identity has been compromised for an unlawful purpose.

- Whether the victim is a resident or the fraudulent transaction occurred here, police officers shall initiate an investigation.
- Officers investigating instances of identity theft will provide victims with information that will assist them in repairing their credit and minimizing the amount of theft.
- Investigating officers will refer to other law enforcement agencies information about fraudulent transactions occurring in their jurisdiction.
- Through a variety of crime prevention programs, the department will educate the public about identity theft and identity theft prevention.

PROCEDURES

A. Definitions

1. **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 but not limited to, 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.
2. **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.

B. Initial Investigation and Reporting

1. Jurisdiction (M.G.L. 266 § 37E): The jurisdiction for an identity theft victim to file a police report is very broad. A victim may file a police report:ⁱ
 - 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.

- d. There are six (6) different action codes to be used when recording an identity theft in the Lexington police log.
 - i. Codes 26A through 26E are 5 different types of Fraud that occurred in Lexington.
 - ii. Code 26Z shall be assigned to a Fraud/Identity Theft case crime that occurred outside of Lexington, but involves a Lexington resident.

Note: A Lexington resident could be subject to identity theft anywhere in or outside the United States. As a service to the resident or local business, Lexington will document the incident and seek to assist the victim contacting an appropriate investigating agency. The 26Z Fraud code will not record this incident as a crime that occurred here in Lexington.

- 2. Identity Theft Reports [42.2.8(a)]
 - a. Police reports and incident numbers contain critical information necessary for victims of identify theft to resolve issues with creditors and credit reporting agencies.
 - b. The report can be used to:
 - i. Lock on a permanent basis information that results from identity theft from appearing on the victim's credit report;
 - ii. Ensure these debts do not reappear on the credit reports;
 - iii. Prevent a company from continuing to collect debts that result from identity theft, or selling them to others for collection; and
 - iv. 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 should be filed prior to the end of the officer's shift, unless unusual circumstances cause it to be filed at a later date.
 - e. A victim shall be provided a copy of the police report within twenty-four hours of its being requested.ⁱⁱ
 - f. Financial institutions often require victims to obtain and forward a police report to them. At a minimum a case number and journal note shall be provided to the victim at the time the identity theft is reported.

C. Assisting the Victim [42.2.8(c)]

1. Resources for Victims

- a. Police officers investigating 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 should provide the victim with current brochures that help to inform victims of identity theft. Officers may also need to assist the victim in the completion of additional forms provided by other resources. These resources may include:
 - i. Dispute letter for new accounts;
 - ii. Dispute letter for existing accounts; and
 - iii. Identity theft affidavit (Federal Trade Commission)

2. Victim Contact with Credit Bureaus

- a. Victims should be advised to contact at least 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 advise the victim to notify 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. This will help the victim when speaking with financial institutions.
7. ID Theft Affidavit: The victim may have an ID Theft Affidavit provided by a financial institution. The victim should be asked to provide the Department with a copy once it has been completed. Completed affidavits should be filed with the case file. [42.2.8(b)]
8. Information Sharing: The officer should inform the victim that information about the case might 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.

D. 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. If possible, these referrals should be done within three days to give the Bureau the best chance of securing financial data and potential security film.
 - b. Upon receiving the referral, the Detective Bureau Commander shall screen and evaluate the case for additional investigative resources. (Solvability factors)
 - i. Cases that show little possibility of being investigated to a successful conclusion may be closed.

42Q-Identity Theft

- ii. Cases, which may be continued further by patrol personnel, shall be returned to the referring officer for further investigation.
 - iii. Cases identified for further investigative follow up by the Detective Bureau shall be assigned to a specific detective by the Lieutenant Detective or in his absence by the Detective Sergeant.
- c. Detectives assigned to investigate will follow up on promising leads which may include:
- i. Determining the point of compromise;
 - ii. Interviewing or causing to be interviewed employees of financial institutions and stores;
 - iii. Securing and preserving images of the suspects;
 - iv. Tracing goods fraudulently purchased;
 - v. Interacting with bank and credit card company fraud departments; and
 - vi. Investigating instances where the victim's identity was used to avoid criminal prosecution.
- d. The victim should be kept apprised of all significant developments in the investigation, and should be contacted in all instances where it is learned that their identity has been further compromised or used.
2. Identity Thefts and Financial Crimes Task Force

The timely sharing of information among law enforcement agencies is critical to the prevention of additional damage to the victim's identity and credit, and to the successful apprehension of the subject(s). Once the officer's report has been approved, the officer's report should be immediately faxed to the Identity Theft and Financial Crimes Task Force in Boston (fax 617-556-0405). Where appropriate, the task force will notify the US Secret Service. The Detective Bureau will typically handle this action. [42.2.8(d)]

3. Referrals from Other Law Enforcement Agencies [42.2.8(d)]

Upon receiving a referral from another law enforcement agency regarding an element of identity theft occurring in this community, this Department will assist other agencies upon request and may initiate an investigation.

4. Dissemination of Surveillance Photographs
 - a. Images of subjects conducting transactions related to identity theft may be shared with other agencies through any of the following:
 - i. State and regional identity theft and counter crime taskforces;
 - ii. Northeastern Massachusetts Law Enforcement Council (NEMLEC) Monthly Detective meetings;
 - iii. New England State Police Information Network (NESPIN); and
 - iv. MassMostWanted.org web site.
 - b. A 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.

E. Prevention and Education [42.2.8(e)]

The Federal trade commission has a variety of identity theft material, available for download at www.ftc.gov.

1. The Lexington Police Department will keep the public informed about identity fraud in general, and specifically about steps people can take to prevent victimization.
2. BROCHURES: Brochures relating to avoiding identity theft are available to the public in the lobby of the station.
3. PUBLIC PRESENTATIONS: The Department will seek out opportunities to provide education and prevention presentations to civic groups.
4. WEB SITE: The Department web site will maintain links to sites that offer information about identity theft.
5. MEDIA: The Department will use the media where appropriate to warn citizens about trends in identity crime.

ⁱ M.G.L. c. 266, §37E.

ⁱⁱ M.G.L. c. 266, §37E.