

		Policy & Procedures			No. 1.44	
		Subject:				
		Identity Theft				
		Issuing Authority:			Effective Date:	Review Date:
		Chief of Police			05/03/2014	10/24/2023
					References:	
Revision & Reissued Dates:	06/01/2016					
	06/24/2018					
	07/24//2020					

CALEA STANDARDS

42.2.8

General Considerations and Guidelines

Purpose Identity theft is the unlawful use of another person's personal information, such as name and date of birth, Social Security number, credit card or account numbers, and passwords, among others, for the purpose of committing fraud or some other form of criminal 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 and of 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, utilities, or medical treatment, 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 or bank 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.

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

- In each case of reported identity crime, whether the victim resides here or a fraudulent transaction occurs here, an officer will conduct an investigation and write a report. **42.2.8 A**

- Specialized report forms will be used by members of this department when required. **42.2.8 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. **42.2.8 C**
- The department will refer to other law enforcement agencies information about fraudulent transactions occurring in their jurisdictions. There will be a coordination of investigations with other agencies when necessary. **42.2.8 D**
- The department will seek to educate the public about the issue of identity crime, including methods for preventing it. **42.2.8 E**
- MGL C266. S37e authorizes police to arrest for the offense of identity fraud if probable cause exists.

Definitions 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, bank account number, credit card number or computer password.

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 Massachusetts General Law C266. S37e.

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 report:
 - a. In the community where the victim resides;
 - b. In the community 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 community where the breach of security occurred in whole or in part.

2. Identity Theft Affidavit

- a. The victim should be provided an Identity Theft Affidavit* from the Federal Trade Commission. (*See Section B under resources)
- b. The form's instructions contain valuable information to the victim and also provides for the capture of the information necessary to meet the requirements of an "Identity Theft Report"; information necessary for police to conduct a thorough investigation.
- c. A completed copy should be obtained and filed with the report written by the officer.

3. Identity Theft Reports

- a. Police reports and incident numbers are critical documents for victims of identity theft to resolve issues with creditors and credit reporting agencies.

The report can be used to:

- Permanently block fraudulent information that results from identity theft from appearing on the victim's credit report;
- Ensure these debts do not reappear on the credit reports;
- Prevent a company from continuing to collect debts that result from identity theft, or selling them to others for collection; and
- Allow victims to place extended fraud alert on their credit report.

B. Assisting the Victim

1. Resources for Victims **42.2.8 C**

- 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, and 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 a variety of reporting forms and advisory materials available from the Federal Trade Commission (FTC) as well as information from Massachusetts and Federal Consumer Assistance websites.

A sampling of documents can be found on the "M Drive" in the folder labeled 'Identity Theft'. They include:

- Identity Theft Complaint & Affidavit

- Attorney General's Guide on Identity Theft for Victims & Consumers
- Annual Credit Report Request Form
- Sample Dispute Letter

2. Victim Contact with Credit Bureaus **42.2.8 C**

Victims should be advised to contact one of the three major credit bureaus and place a *fraud alert* on their credit report. 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.

The three credit bureaus are:

- 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 Information Solutions
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: 1-800-680-7289
www.transunion.com

3. Notifications to Financial Institutions

The officer should ensure that the victim notifies each financial institution where they have an account, so the 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.ftc.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 institute where their identity has been compromised. They should be advised to keep a record of all correspondence and conversations with financial institutions and other companies, credit bureaus, and law enforcement officials. All correspondences should be sent by certified mail, return receipt requested, to document what the company received and when. Copies should be kept of everything.

C. Follow-up Investigation

1. Initial Follow-up

Cases that require an in-depth investigation may be referred to the Criminal Investigations Unit for follow-up.

Investigators should follow-up on promising leads which may include:

- Determining the point of compromise;
- Interviewing or causing to be interviewed employees of financial institutions and stores;
- Securing and preserving images of the suspects;
- Tracing goods fraudulently purchased;
- Interacting with bank and credit card company fraud departments; and
- Investigating instances where the victim's identity was used to avoid criminal prosecution.

Investigations which lead to another jurisdiction shall be coordinated with the appropriate federal, state, or local law enforcement agency. **42.2.8 D**

The regional IRS CI contact for identity theft matters is Special Agent Kevin Millen. SA Millen can be contacted at (860) 756-4719.

Investigators shall keep victims apprised of all significant developments in the investigation, and shall contact them in all instances where it is learned that their identity had been further compromised or used.

2. Referrals from Other Law Enforcement Agencies **42.2.8 D**

Referrals of identity theft from outside agencies may be received by our department. Investigators shall coordinate investigative efforts with the referring agency. This may include:

- Following-up on all leads as requested by the referring agency;
- Documenting all fraudulent transactions;
- Securing all available evidence, including photographs, stolen property, and relevant documents;
- Informing the referring agency, officer or agent of all significant developments in the investigation; and
- 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

Images of subjects conducting transactions related to identity theft may be shared with other agencies. Investigators should also view images received from other sources to determine if a subject has committed crimes in other jurisdictions.

D. Prevention and Education 42.2.8 E

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.

- The department's web site will maintain links to sites that offer information about identity theft.
- When requested, members of the Family Services Unit or the Criminal Investigations Unit will offer education and prevention programs for community groups and educational institutions.