IDENTITY THEFT

WILLIAMSTOWN POLICE DEPARTMENT POLICY & PROCEDURE NO. **2.16**	ISSUE DATE: 12/10/2021
	EFFECTIVE DATE: 12/10/2021
MASSACHUSETTS POLICE ACCREDITATION STANDARDS REFERENCED: **42.2.8**	REVIEW / REVISION DATE: 12/10/2022

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 local instances (when and where appropriate) 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, police personnel will conduct an investigation if warranted and open a log entry to document same. If applicable, the report will be transferred to another agency.

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

A.1. JURISDICTION: The jurisdiction for an identity theft victim to file a police report is very broad. A victim may file a police report: [i]

A.1.a. In any municipality where the victim resides;

A.1.b. In any municipality 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

A.1.c. In the municipality where the breach of security occurred in whole or in part.

A.2. IDENTITY THEFT LOG ENTRIES **[42.2.8(A)]**

A.2.a. Log entries and at times incident numbers are critical documents for victims of identity theft to resolve issues with creditors and credit reporting agencies.

A.2.b. The report can be used to:

A.2.b.1) Permanently lock fraudulent information that results from identity theft from appearing on the victim's credit report;

A.2.b.2) Ensure these debts do not reappear on the credit reports;

A.2.b.3) Prevent a company from continuing to collect debts that result from identity theft, or selling them to others for collection; and

A.2.b.4) Allow a victim to place an extended fraud alert on his or her credit report.

A.2.c. The report must contain details about the accounts and inaccurate information that resulted from the identity theft.

A.2.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.

A.2.d.1) The victim's copy of an Investigative Case Report Form will meet the time requirements for the purpose of reporting.

A.2.d.2) The officer's report should also be submitted.

A.2.e. A victim shall be provided a copy of the police report within twenty-four hours of its being requested.[ii]

A.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)]

B.1. RESOURCES FOR VICTIMS

B.1.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.1.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:

B.1.b.1) Dispute Letter for New Accounts;

B.1.b.2) Dispute Letter for Existing Accounts;

B.1.b.3) Identity Theft Affidavit (Federal Trade Commission]; and

B.1.b.4) Referral to www.IdentityTheft.gov for resources.

B.2. VICTIM CONTACT WITH CREDIT BUREAUS

B.2.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.2.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

B.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.

B.4. FEDERAL TRADE COMMISSION: www.IdentityTheft.gov is the federal government's one-stop resource for identity theft victims to report the crime to the FTC and get recovery help. www.IdentityTheft.gov asks victims about the identity theft. Based on the answers, the site will:

Build a personal recovery plan and walk the victim through each recovery step.

Create an Identity Theft Report that victims can use in place of a police report in most cases. This report helps clear their credit reports of fraudulent information.

Generate personalized letters and forms those victims can send to debt collectors, credit agencies, and others to help resolve the identity theft.

IdentityTheft.gov has detailed recovery steps for more than 30 types of identity theft. Officers will have access to victims' reports through the Consumer Sentinel Network.

B.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.

B.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.

B.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.

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

C.1. INITIAL FOLLOW-UP

C.1.a. The primary case officer shall follow up on promising leads which may include:

C.1.a.1) Determining the point of compromise;

C.1.a.2) Interviewing or causing to be interviewed employees of financial institutions and stores;

C.1.a.3) Securing and preserving images of the suspects;

C.1.a.4) Tracing goods fraudulently purchased;

C.1.a.5) Interacting with bank and credit card company fraud departments; and

C.1.a.6) Investigating instances where the victim's identity was used to avoid criminal prosecution.

C.1.b. Investigations which lead to another jurisdiction shall be coordinated with the appropriate federal, state, or local law enforcement agency.

C.1.c. Officers 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.

C.2. REFERRALS FROM OTHER LAW ENFORCEMENT AGENCIES **[42.2.8(D)]**

C.2.a. Referrals of identity theft from outside agencies will normally be assigned to an officer.

C.2.b. Upon receiving a referral, the officer shall coordinate investigative efforts with the referring agency. This may include:

C.2.b.1) Following-up on all leads as requested by the referring agency;

C.2.b.2) Documenting all fraudulent transactions;

C.2.b.3) Securing all available evidence, including photographs, stolen property, and relevant documents;

C.2.b.4) Informing the referring agency, officer or agent of all significant developments in the investigation; and

C.2.b.5) Preparing a comprehensive report of the follow-up investigation and providing a copy to the referring law enforcement agency or official.

C.3. DISSEMINATION OF SURVEILLANCE PHOTOGRAPHS

C.3.a. Images of subjects conducting transactions related to identity theft may be shared with other agencies through:

C.3.a.1) State and regional identity theft and counter crime taskforces;

C.3.a.2) New England State Police Network; and

C.3.a.3) MassMostWanted.org web site.

C.3.b. The officer 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.

C.4. THE FEDERAL TRADE COMMISSION CONSUMER SENTINEL NETWORK: A POWERFUL INVESTIGATIVE TOOL

A law enforcement-only database of more than 15 million consumer reports about identity theft, imposter scams, and other consumer fraud. Use it to investigate fraud-based crimes, get aggregate data for your jurisdiction, and connect with law enforcers nationwide.

Search by full or partial company names, phone numbers, addresses, and more;

Use visualization tools to explore links between companies, locations, phone numbers, emails, and URLs;

Identify suspects and witnesses;

Get top violator reports for your jurisdiction;

See complaint trends in your jurisdiction.

Register at https://Register.ConsumerSentinel.gov

D. Prevention and Education [42.2.8(e)]

[IDENTITY THEFT MATERIALS ARE AVAILABLE TO DOWNLOAD FROM THE FEDERAL TRADE COMMISSION.]

D.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.

D.2. BROCHURES: The department will make brochures relating to avoiding identity theft available to the public.

D.3. WEB SITE: The department web site will maintain links to sites that offer information about identity theft.

D.4. MEDIA: The department will utilize 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.