	MEDFIELD POLICE DEPARTMENT	**POLICY NO. 2.07**

IDENTITY THEFT

MASSACHUSETTS POLICE ACCREDITATION STANDARDS REFERENCED: **42.2.8, 82.2.4**	DATE OF ISSUE: 06/04/2023 EFFECTIVE DATE: 06/04/2023 REVISION DATE: 11/07/2025
ISSUING AUTHORITY: Michelle Guerette Chief of Police	

BACKGROUND:

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.

POLICY:

The Medfield Police Department will investigate and file a report in all instances where a citizen's identity has been compromised for an unlawful purpose and the victim resides in Medfield or a fraudulent transaction occurs in Medfield. Information or reports involving fraudulent transactions occurring in other jurisdictions will be referred to the appropriate law enforcement agency.

The Department will seek to educate the public about the issue of identity crime, including methods for preventing it. 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.

PROCEDURES:

All reports of identity crime will be investigated by a police officer and 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. 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.

Theft of a Credit Card [42.2.8(a)]

An officer investigating the theft of a credit card will attempt to determine how the subject obtained the credit card, and must list in the report the names and account numbers of the credit cards involved.

Point of Compromise [42.2.8(a)]

An officer investigating the unauthorized use of the victim's identity to commit a financial crime will attempt to determine the point where the victim's identity was compromised.

Determining the point of compromise will assist the officer in learning important information about the subject's MO, and may lead him or her to other victims.

If the point of compromise is outside the Town of Medfield, the officer will pass relevant information on to the appropriate law enforcement agency. All such referrals must be documented in the officer's report, including:

1. The law enforcement agency to which the referral was made;
2. The name of the officer to whose attention the referral was sent; and
3. The method by which the officer's report was transmitted (mail, fax, email, etc.)

Financial Transactions [42.2.8(a)]

The officer taking the report of identity theft must attempt to identify any financial transactions that have been made using the victim's identity and take proper steps to preserve evidence, including:

1. Interviewing or causing to be interviewed employees of stores or banks that waited on the subject using the identity;

2. Determining whether purchases or transactions were photographed or videotaped, and securing or causing to be secured any resulting photographs, tapes or other images;

3. In the case of banking transactions, obtain and include in the police report the names and branches of the financial institution(s), the name on the account(s), the type of account and account number(s) involved, the amount of loss; and the location of the unlawful transaction; and

4. If the victim's identity has been used to apply for a fraudulent loan, obtain information about the application and trace the goods purchased with the loan.

Criminals Avoiding Capture [42.2.8(a)]

In some cases a victim's identity will be used by a criminal to avoid apprehension or prosecution. In all such cases, the investigating officer should document where and when the subject used the victim's identity, and notify the law enforcement agencies that filed charges against the victim based upon the subject's fraudulent use of their personal information.

Identity Theft and Financial Crimes Task Force

The timely sharing of information among law enforcement agencies is critical to the prevention of further damage to the victim's identity and credit, and to the successful apprehension of the subject(s). When appropriate, officers may fax approved reports 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. **[82.2.4]**

Initial Follow-up

Cases of identity theft that require an in-depth investigation beyond that which can be conducted by the investigating patrol officer must be forwarded to the Department's Investigative Bureau for follow-up. **[82.2.4]**

Detectives investigating cases of identity theft shall follow-up on unresolved leads in the patrol officer's report, including but not limited to determining the point of compromise, interviewing or causing to be interviewed employees of financial institutions and stores, securing and preserving images of the subject, tracing goods fraudulently purchased and investigating instances where the victim's identity was used to avoid criminal prosecution.

If a detective learns of an unlawful transaction or delivery of goods outside the Town of Medfield, he shall coordinate with the appropriate federal, state, or local law enforcement agency, or with the Identity Theft and Financial Crimes Task Force in Boston (617-556-4400), to investigate the transaction or delivery, and if possible, recover fraudulently obtained goods. **[42.2.8(d)]**

The detective should contact the Identity Theft and Financial Crimes Task Force to determine whether the case can be linked to other investigations. The task force maintains an extensive database of information concerning identity fraud that includes telephone numbers used by subjects and "hot addresses" where fraudulently obtained goods have been shipped.

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.

Referrals from Other Law Enforcement Agencies

Upon receiving a referral from another law enforcement agency regarding an element of identity theft occurring in Medfield, detectives shall:

1. Follow-up on all leads as requested by the referring agency;

2. Document all fraudulent transactions occurring in the Town of Medfield;

3. Secure all available evidence including photographs, stolen property, and relevant documents;

4. Inform the referring agency, officer or agent of all significant developments in the investigation; and

5. Prepare a comprehensive report of the follow-up investigation, and provide a copy to the referring law enforcement agency or official.

Dissemination of Surveillance Photographs

In all cases where photographs or images of subjects conducting transactions related to identity theft are available, the investigating detective will ensure that the images are posted on the MassMostWanted.org web site in a timely fashion. The detective should also compare the images with others posted on the web site to determine whether the subject has committed crimes in other jurisdictions.

Resource Guide for Victims

Police officers investigating an identity theft must not only attempt to identify the subjects responsible, but also assist the victim in minimizing the damage done. An officer investigating an identity theft must provide the victim with a copy of the Department's document, "Identity Theft, a Resource Guide" and should record his name and the case number on the cover of the resource guide. **[42.2.8(c)]**

Victim Contact with Credit Bureaus

The officer should advise the victim to contact one of the three major credit bureaus and place a fraud alert on their credit reports. The credit bureaus are required to share

information with each other about identity theft, so there is no need for the victim to contact more than one of them. Victims may also request a copy of their credit report. 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

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.

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 https://www.identitytheft.gov .

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

Documenting Contacts

The officer should advise the victim to maintain a log detailing each instance where his identity has been compromised, and each contact he makes with a financial institution, credit bureau, store, or law enforcement agency.

ID Theft Affidavit

The victim must be provided a blank ID Theft Affidavit, and be asked to provide the Department with a copy once it has been completed. Completed affidavits should be filed with the case.

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.

The Medfield Police 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 through the Department web site, and the use of other media where appropriate, to warn citizens about trends in identity crime. **[42.2.8(e)]**