


NORTHAMPTON POLICE DEPARTMENT Administration & Operations Manual		
Policy: Identity Theft and Fraud		AOM: O-427
Massachusetts Police Accreditation Standards Referenced: [42.2.1], [42.2.8.a], [42.2.8.c], [42.2.8.d], [42.2.8.e]		Issuing Authority <hr/> John D. Cartledge Chief of Police
Dissemination Date: 07/10/2006	Amended: 12/08, 3/11, 3/13, 8/23	
Effective Date: 08/01/2006	Reviewed: 12/08, 3/11, 3/13, 3/15, 3/17, 6/19, 8/23, 3/26	

Table of Contents

I. Purpose 1

II. Policy..... 1

III. Definitions.....1

IV. Procedures 2

I. Purpose

The purpose of this policy is to provide employees with protocols for accepting, recording, and investigating the crime of identity theft.

II. Policy

Identity theft and fraud is one of the fastest growing and most serious economic crimes in the United States for both financial institutions and persons whose identifying information has been illegally used. Identity theft and fraud is also a tool that terrorists and those who are attempting to evade the law can use to their advantage. Therefore, this police agency shall take those measures necessary to record criminal complaints, assist victims in contacting other relevant investigative and consumer protection agencies, and work with other federal, state, and local law enforcement and reporting agencies to identify perpetrators.

III. Definitions

Identity theft is the wrongful use of another person’s identifying information such as credit card, social security or driver’s license numbers, to commit financial or other

crimes. Identity theft is generally a means for committing other offenses such as fraudulently obtaining financial credit or loans, among other crimes.

IV. Procedures (42.2.1)

A. Legal Prohibitions:

1. Identity theft is punishable under federal law “*when any person knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a felony under any applicable state or local law*”. [18 U.S.C. § 1028 (a) (7)].
2. Identity theft is punishable under state law, M.G.L.c.266 sec. 37E (Misdemeanor). However, statutory authority is given under subsection (e) of this section for arrest on probable cause for the offense of identity fraud.

B. Taking Crime Reports: [42.2.8,a]

All sworn police personnel are authorized to take crime reports on identity theft. Recording all relevant information and data in such reports is essential to further an investigation. Therefore, officers and/or supervisors should;

1. Fully record information concerning criminal acts that may have been committed by illegally using another’s personal identity as covered by state and federal law.
2. Obtain or verify as appropriate, identifying information of the victim to include; date of birth, social security number, driver’s license number, other photograph identification, current and most recent prior addresses, and telephone numbers.
3. Document the nature of the fraud or other crime committed in the victim’s name.
4. Determine what types of personal identifying information may have been used to commit these crimes (i.e., social security number, driver’s license number, credit card numbers, etc.) and whether any of these have been lost, stolen or potentially misappropriated.
5. Document any information concerning where the crime took place, the financial institutions or related companies involved and the residence or whereabouts of the victim at the time of these events.
6. Determine whether the victim authorized anyone to use their name or personal information.
7. Determine whether the victim has knowledge or belief that specific person or persons have used their identity to commit fraud or other crimes.
8. Determine whether the victim is willing to assist in the prosecution of suspects identified in the crime.
9. Determine if the victim has filed a report of the crime with other law enforcement agencies and whether such agency provided the complainant with a report number.
10. If not otherwise provided, document and describe the crime, the documents or information used, and the manner in which the victim’s identifying information was obtained.
11. Forward the report through the chain of command to appropriate investigative officers.

C. Assisting Victims: [42.2.8,c]

Officers taking reports of identity theft should take those steps reasonably possible to help victims resolve their problem. This includes providing victims with the following suggestions where appropriate.

1. Contact the Federal Trade Commission (FTC) for information and assistance related to identity theft crimes at 1-877-IDTHEFT.
2. Cancel each credit and charge card and request new cards with new account numbers.
3. Contact the fraud departments of the three major credit-reporting agencies (Equifax at 1-800-525-6285, Experian at 1-888-397-3742, and TransUnion at 1-800-680-7289).
 - a. Ask that a fraud alert to be placed on the account and add a victim's statement requesting creditors to contact the victim before opening new accounts in their name. The victim should also request copies of their credit report.
4. If bank accounts are involved, report the loss to each financial institution. Cancel existing accounts and open new ones with new account numbers. If deemed necessary, place stop payments on outstanding checks and contact creditors to explain.
5. If a driver's license is involved, contact the state motor vehicle department. If the driver's license uses the social security number, request a new driver's license number. In such cases, also check with the Social Security Administration to determine the accuracy and integrity of your account.
6. Change the locks on your house and cars if there is any indication that these have been copied or otherwise compromised.

D. Investigations: [42.2.8,d]

Investigation of identity theft should include but not be limited to the following actions where appropriate.

1. Review the crime report and conduct any follow-up inquiries of victims or others as appropriate for clarification/expansion of information.
2. Contact the FTC Consumer Sentinel Law Enforcement Network and search the database for investigative leads.
3. Contact other involved or potentially involved law enforcement agencies for collaboration and avoidance of duplication. These agencies include but are not limited to;
 - a. Federal Bureau of Investigations
 - b. U. S. Secret Service
 - c. U.S. Postal Inspection Service

- d. Massachusetts State Police Investigative Units
- e. Local police agencies

E. Community Awareness and Prevention: [42.2.8,e]

When officers engaged in public education/information forums, community crime prevention, and awareness presentations, or similar speaking or information dissemination efforts, they should provide the public with information on the nature and prevention of identity theft.