
	GAITHERSBURG POLICE DEPARTMENT		
	Identity Theft Investigation and Reporting		
	GENERAL ORDER	610.2	
Effective Date	05/26/2015		
Authorized by:	Mark P. Sroka CHIEF OF POLICE	SIGNATURE	DATE

I. DEPARTMENT POLICY

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

The Department 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 offenders.

II. LAWS AND REPORTING PROCEDURES

A. Legal Prohibitions

1. Identity theft is punishable under federal law [18 U.S.C. Sect. 1028 (a)(7)] “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.

2. Identity theft is punishable under state law [MD Criminal Law Article Sect. 8-301] “A person may not knowingly, willfully, and with fraudulent intent possess, obtain, or help another to possess or obtain any personal identifying information of an individual, without the consent of the individual, in order to use, sell, or transfer the information to get a benefit, credit, good, service, or other thing of value in the name of the individual; a person may not knowingly and willfully assume the identity of another to avoid identification, apprehension, or prosecution for a crime; or with fraudulent intent to get a benefit, credit, good, service, or other thing of value; or avoid the payment of debt or other legal obligation.

B. Reporting Procedures

1. All sworn personnel are authorized and required to document event reports on identity theft. Recording all relevant information and data in such reports is essential to further the investigation.

Therefore, all officers and/or supervisors shall:

- a. Fully record information concerning criminal acts that may have been committed by illegally using another's personal identity as stated in federal and state law.
- b. Use appropriate UCR classifications for identity theft and other fraudulent acts committed against an individual when there is evidence that the following types of unauthorized activities have taken place in the victim's name:
 - Credit card charges, debit cards, ATM cards;
 - Credit card checks written against their accounts;
 - Credit card accounts opened or account addresses changed;
 - Establishment of a line of credit at a store or obtaining a loan at a financial institution;
 - Goods or services purchased in their name;
 - Gaining access to secure areas; and
 - Used in computer fraud crimes.
- c. Document the crime on an event report with the appropriate classification, as there are no specialized report forms for this crime in Montgomery County.
- d. Document the nature and location of the fraud or other crimes committed in the victim's name in the narrative of the report.
- e. Determine what types of personal identifying information may have been used to commit these crimes (i.e., social security number, driver's license number, birth certificate, credit card numbers and corporation of issuance) and whether any of these have been lost, stolen or potentially misappropriated.
- f. Determine whether the victim authorized anyone to use his/her name or personal information.

- g. Determine whether the victim has knowledge or belief that the specific person or persons have used his/her identity to commit fraud or other crimes.
- h. Determine if the victim has filed a report of the incident(s) with other law enforcement agencies and whether such agency provided a report or complaint number to the victim.

C. Investigative Responsibilities

- 1. Investigations of identity theft shall be forwarded to the Montgomery County Police Fraud Unit for investigative follow up. Sworn personnel may conduct follow up investigations with approval from their immediate supervisor, bureau commander or the MCP Fraud Unit commander as deemed appropriate. Investigations of identity theft shall include but not be limited to the following:
 - a. Review the initial event report and conduct any follow up inquires of victims or appropriate witnesses for clarification/expansion of the original incident.
 - b. Contact the FTC (Federal Trade Commission) Consumer Sentinel law enforcement network and search the database for investigative leads.
 - c. Contact other appropriate law enforcement agencies for collaboration and avoidance of duplicated efforts. These agencies include:
 - Federal law enforcement agencies such as the US Secret Service, the FBI, and the US Postal Inspectors;
 - Other allied Maryland agencies to include the Maryland State Police; and
 - Any other state or local law enforcement agencies where the victim has filed a crime report or where there is an indication that the identity theft occurred.

D. Assisting Victims

- 1. Officers taking reports of identity theft should take those steps reasonably possible to help victims resolve their problem or

complaint. This includes providing victims with the following information through personal contact or in written brochure forms where appropriate.

- Contact the FTC (Federal Trade Commission) hotline at the number listed for them in the General Orders Phone Number WIP.xlsx which acts as the national clearinghouse for information related to identity theft crimes, for assistance from trained counselors in resolving credit related problems.
- Cancel each credit, debit or charge card and request new cards with new account numbers.
- Contact the fraud departments of the three major credit reporting agencies and ask them to put a fraud alert on the account and add a victim statement requesting creditors to contact the victim before opening new accounts in his/her name. Also request copies of your credit report.
- 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 any outstanding checks and contact creditors to explain.
- If driver's licenses are involved, contact the State of issuance department of motor vehicles to report the loss or theft of license number.
- If Social Security card or numbers are involved, contact the Social Security Administration to obtain a new card or new numbers.
- If appropriate, change the locks on your house and cars if these may have been copied or otherwise compromised.

E. Public Information and Prevention

1. Where reasonable and appropriate, officers engaged in public education or information forums, crime prevention and awareness presentations or similar speaking or information dissemination efforts should provide the public with information on the nature and prevention of identity theft. These efforts will be coordinated by the Community Services Office at the approval of the Special Operations Bureau commander. A report of speaking engagements will be forwarded to the Office of the Chief of Police.

2. The department makes available to the public a pamphlet with information about Identity Theft prevention.

F. National Security Coordination with Other Agencies

1. When appropriate and if the initial reporting officer determines that the nature of the identity theft may be related to terrorist activity or other national security interests, the officer shall contact the FBI Joint Terrorism Task Force (JTTF), Baltimore Field Division at the number listed for them in the General Orders Phone Number WIP.xlsx and forward all appropriate event reports and field notes to the JTTF agent or officer on duty. In the event that the JTTF does not respond, the officer or supervisor will contact the Department's Investigative Section or Special Operations Bureau Commander for follow up contact and notification.
2. The Federal Trade Commission hotline is another appropriate avenue to exchange and provide for coordination of investigations with other agencies.