Lexington Police Department

Lexington, Kentucky

SPECIAL ORDER

BY THE AUTHORITY OF THE CHIEF OF POLICE

S.O. 2010-01 **Identity Theft**

Rescinds: NA
References: CALEA Chapter(s) 42

Effective Date: 01/26/10
Distribution Code: B | All Department Employees

Originally Issued: 2010

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 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. The Lexington Division of Police 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. PROCEDURES

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 and state law. [18 U.S.C. § 1028(a)(7)] Enforcement under this provision will only be carried out in conjunction with federal authorities.

2. Identity theft is punishable under state law KRS 514.160 which states a person is guilty of the theft of the identity of another when he or she knowingly possesses or uses any current or former identifying information of the other person or family member or ancestor of the other person, such as that person's or family member's or ancestor's name, address, telephone number, electronic mail address, Social Security number, driver's license number, birth date, personal identification number or code, and any other information which could be used to identify the person, including unique biometric data, with the intent to represent that he or she is the other person for the purpose of:

(a) Depriving the other person of property;
(b) Obtaining benefits or property to which he or she would otherwise not be entitled;
(c) Making financial or credit transactions using the other person's identity;
(d) Avoiding detection; or
(e) Commercial or political benefit.

B. Taking Crime Reports

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 investigation. Therefore, officers shall:

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. Classify as identity theft 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.

a. Credit card accounts opened or account addressed changed.

b. Establishment of a line of credit at a store or obtaining a loan at a financial institution.

c. Goods or services purchased in their name.

d. Gaining access to secure areas.

e. Used as computer fraud.

3. Obtain or verify as appropriate identifying information of the victim to include date of birth, social security number, driver's license number, other photo identification, current and most recent prior addresses, and telephone numbers.

4. Document the nature of the fraud or other crime committed in the victim's name.

5. 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 state of issuance, etc.) and whether any of these have been lost, stolen or potentially misappropriated.

6. 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.

7. Determine whether the victim authorized anyone to use his or her name or personal information.

8. Determine whether the victim has knowledge or belief that specific person or persons have used his or her identity to commit fraud or other crimes.

9. Determine whether the victim is willing to assist in the prosecution of suspects identified in the crime.

10. Determine if the victim has filed a report of the crime with other law enforcement agencies. If the victim has previously reported the crime to another law enforcement agency, a duplicate report is unnecessary. In these situations, the officer should record the contact and relevant information

on a Division memoranda and refer the victim to the Bureau of Investigation Financial Crimes Unit.

11. If not otherwise provided, document/describe the crime, the documents or information used, and the manner in which the victim's identifying information was obtained.

12. Should the identity theft have potential national security implications, the reporting officer should contact agency intelligence personnel immediately to ensure timely dissemination to other appropriate authorities.

C. Assisting Victims

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) (1-877-IDTHEFT)—which acts as the nation's clearinghouse for information related to identity theft crimes—for assistance from trained counselors in resolving credit related problems.

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 (1-800-525-6285), Experian (1-888-397-3742), TransUnion (1-800-680-7289)], and ask them to put a fraud alert on the account and add a victim's statement requesting creditors to contact the victim before opening new accounts in his or her name. Additionally, victims may want to request copies of their credit report and examine them for fraudulent activity and accounts. Records pertaining to fraudulent transactions involving the victims information/accounts are available to the victim pursuant to Section 609(e) of the Fair Credit Reporting Act [15 U.S.C. § 1681(g)]. A form letter to request for fraudulent transaction/account information is available through the Federal Trade Commission website as well as the Division of Police website.

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 their 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

Investigation of identity theft shall 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 other involved or potentially involved law enforcement agencies for collaboration and avoidance of duplication. These agencies include but are not limited to

a. Federal law enforcement agencies such as the U.S. Secret Service, the Federal Bureau of Investigation, and the U.S. Postal Inspection Service as appropriate whether or not the victim has filed a crime report with them.

b. Any state and/or local enforcement agency with which the victim has filed a crime report or where there is an indication that the identity theft took place.

E. Community Awareness and Prevention

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

1. Identity theft awareness/prevention information will be made available through the agency website.