

Model Policy

<i>Effective Date</i> January 2002		<i>Number</i>
<i>Subject</i> Identity Theft		
<i>Reference</i>		<i>Special Instructions</i>
<i>Distribution</i>	<i>Reevaluation Date</i>	<i>No. Pages</i> 3

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. Also a tool that terrorist 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: 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

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 con-

stitutes a felony under any applicable state or local law and state law. [18 U.S.C. § 1028(a)(7)]

2. Identity theft is punishable under state law (Note: insert state law or state law reference here) _____ which makes a crime to.

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 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. 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 charges, debit cards, ATM cards.
 - b. Credit card checks written against their account.
 - c. Credit card accounts opened or account addressed changed.
 - d. Establishment of a line of credit at a store or obtaining a loan at a financial institution.
 - e. Goods or services purchased in their name.
 - f. Gaining access to secure areas.
 - g. Used as computer fraud.
3. Obtain or verify as appropriate identifying information of the victim to include date of birth, social security number, drivers 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 and whether such agency provided the complainant with a report number.
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. Forward the report through the chain of command to appropriate investigative officers and immediately to intelligence agencies and federal agencies, if it appears to have national security implications.

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. Also request copies of your 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

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 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 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.

This project was supported by Grant No. 2000-DD-VX-0020 awarded by the Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice. The Assistant Attorney General, Office of Justice Programs, coordinates the activities of the following program offices and bureaus: the Bureau of Justice Assistance, the Bureau of Justice Statistics, National Institute of Justice, Office of Juvenile Justice and Delinquency Prevention, and the Office of Victims of Crime. Points of view or opinions in this document are those of the author and do not represent the official position or policies of the U.S. Department of Justice or the International Association of Chiefs of Police.

Every effort has been made by the IACP National Law Enforcement Policy Center staff and advisory board to ensure that this model policy incorporates the most current information and contemporary professional judgment on this issue. However, law enforcement administrators should be cautioned that no "model" policy can meet all the needs of any given law enforcement agency. Each law enforcement agency operates in a unique environment of federal court rulings, state laws, local ordinances, regulations, judicial and administrative decisions and collective bargaining agreements that must be considered. In addition, the formulation of specific agency policies must take into account local political and community perspectives and customs, prerogatives and demands; often divergent law enforcement strategies and philosophies; and the impact of varied agency resource capabilities, among other factors.