



Eric Hawkins
Chief of Police

ALBANY, NEW YORK
POLICE DEPARTMENT
165 HENRY JOHNSON BOULEVARD
ALBANY, NEW YORK 12210



1789

IDENTITY CRIMES
GENERAL ORDER NO: 3.1.50

Issue Date: October 25, 2015	Effective Date: September 19, 2014
Revision Date: September 19, 2014	CALEA:
Volume 3: Operations	Chapter 1: Patrol and Investigations
Distribution: Sworn Personnel	NYSLEAP: 43.1
Issuing Authority: Chief Eric Hawkins	Page: 1 of 4

PURPOSE: The purpose of this policy is to establish policies and procedures for investigating and recording identity theft crimes.

POLICY: It is the policy of the Albany Police Department to take the necessary measures to record identity theft complaints, assist victims in contacting other relevant investigative and consumer protection agencies, provide training for its officers in investigating identity theft crimes, and work with federal, State and other local law enforcement, as well as other reporting agencies to identify perpetrators.

DEFINITIONS: **Identity Theft** – Identity theft means the wrongful use of another person’s identifying information, such as, but not limited to, their credit card, social security number, drivers license, etc., 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.

I. LEGAL PROHIBITIONS

- A. Per, [§ 1028, chapter 47 of title 18](#), of the United States Code, it is a federal crime to knowingly transfer or use, 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 violation of Federal law, or that constitutes a felony under any applicable State or local law.
- B. Identity theft is punishable under the New York State Penal Law, [Article 190](#), which makes it a crime to use personal information to fraudulently obtain credit, goods, services, or other property.
- C. Within the guidelines above, identity theft should be classified as fraudulent when it is committed against an individual and there is evidence that unauthorized activities have taken place in the victim’s name/personal information, such as:
 - 1. Credit card, debit card, or ATM card transactions/withdrawals;
 - 2. Credit card checks written against the victim’s account;
 - 3. Credit card accounts opened/account information amended;
 - 4. Establishment of a line of credit at a store or obtaining a loan at a financial

- institution;
- 5. Goods or services purchased in the victim's name;
- 6. Gaining access to secure areas; or
- 7. Related computer frauds.

II. PROCEDURES

A. When investigating identity theft complaints, officers shall complete a Standardized Incident Report (SIR), according to the following:

1. Record all relevant information and data concerning acts that may have been committed by illegally using another's personal identity, as covered by New York State and Federal law.
 - a. Additional information shall be recorded on a Supplemental Report or an Investigation Report, as applicable.
2. Obtain the victim's identifying information to include the victim's date of birth, social security number, driver's license number, other photo identification, current and prior addresses, and telephone numbers.
3. Document the nature of the fraud or other crimes committed in the victim's name.
4. Determine what types of personal identifying information may have been used to commit these crimes (e.g., 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.
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 his or her name or personal information.
7. 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.
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/describe the crime, the documents or information used, and the manner in which the victim's identifying information was obtained.

III. VICTIM ASSISTANCE

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

1. Contact the Federal Trade Commission (FTC) at 877-IDTHEFT.

- a. The FTC 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 (3) major credit reporting agencies:
 - a. Equifax (1-888-766-0008);
 - b. Experian (1-888-397-3742); and
 - c. Trans-Union (1-800-680-7289).
 - i. Ask the victim to put a fraud alert on their account and add a victim's statement requesting creditors to contact the victim before opening new accounts in his or her name; and
 - ii. Have the victim 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.
 - a. If the driver's license uses the social security number, request a new driver's license number.
 - b. In such cases, also have the victim check with the Social Security Administration to determine the accuracy and integrity of their account.
6. If there is any indication that keys may have been copied or otherwise compromised, recommend that the victim change the locks to their house and vehicles, as applicable.
7. Personnel may refer to [General Order 2.5.15 – Victim/Witness Assistance](#) for further information.

IV. FOLLOW UP INVESTIGATIONS

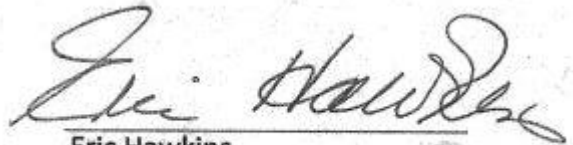
- A. Follow-up investigations of identity thefts shall include, but not be limited to the following:
 1. Detectives shall review incident reports and conduct any follow-up inquiries of the victims or others, as appropriate for clarification/expansion of information.
 2. Contact the [FTC Consumer Sentinel Network](#) for law enforcement agencies 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 the following:
 - a. Federal law enforcement agencies such as the U.S. Secret Service,

the Federal Bureau of Investigation, and the U.S. Postal Inspection Service, whether or not the victim has filed an incident report with them.

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

V. COMMUNITY AWARENESS AND PREVENTION

- A.** The Neighborhood Engagement Unit (NEU) shall incorporate crime prevention and awareness presentations, or similar speaking, or informational dissemination efforts into their crime prevention program to provide the public with information on the nature and prevention of identity theft.



Eric Hawkins
Chief of Police