



University of Pennsylvania Police Department 4040 Chestnut Street, Philadelphia, Pa 19104		 
Directive: 92	Subject: Identity Crimes	Effective Date: 01/05/2007
Order of: Gary Williams, Chief of Police		Amended Date: 08/01/2023

I. Purpose

This directive will serve as a guideline to officers and detectives of the University of Pennsylvania Police Department (UPPD) who may be required to take initial reports and conduct follow-up investigations relative to identity crimes.

II. Policy

It shall be the policy of the UPPD to document and thoroughly investigate reports of identity crimes. Technological advantages in society coupled with the need for conveniences have contributed to a relatively new and devastating type of criminal activity; namely identity crimes. These crimes entail the illegal use of personally identifiable information to facilitate various frauds and unlawfully obtain goods, services, and financial gain. Identity crimes are difficult to track and often involve criminals who are more technologically skilled and geographically diverse. Working with our partners in the Philadelphia Police Department and other federal, state and local law enforcement entities the UPPD will diligently document and investigate crimes of this nature reported to our department.

III. Scope

This directive shall affect all sworn employees.

IV. Definitions

A. Essential elements of Identity Theft (18 PA C.S. Sec. 4120)

1. Offense Defined

- a. A person commits the offense of identity theft of another person if he **possesses** or uses, through any means, **identifying information** of another person without the consent of that other person to further any unlawful purpose.
- b. Separate offenses – Each time a person possesses or uses identifying information in violation of subsection (a) constitutes a separate offense under this section. However,

the total values involved in offenses under this section committed pursuant to one scheme or course of conduct, whether from the same victim or several victims, may be aggregated in determining the grade of the offense.

2. Identifying information defined

- a. Any **document**, photographic, pictorial or computer image of another person, or any fact used to establish identity, including, but not limited to, a name, birth date, Social Security number, driver's license number, non-driver governmental identification number, telephone number, checking account number, savings account number, student identification number, employee or payroll number or electronic signature.

3. Venue

- a. The Pennsylvania Identity Theft Statute indicates that the venue for an identity theft is as follows:
 - 1) The **residence of the person** whose identifying information has been lost or stolen or has been used without the person's consent.
 - 2) The **place** where a person **used or possessed** the identifying information of another without the other's consent to further any unlawful purpose; or
 - 3) The **business or employment address of the person** whose identifying information has been lost or stolen or has been used without the person's consent, if the identifying information at issue is associated with the person's business or employment.

4. Definitions

- a. **Document** - Any writing, including, but not limited to, birth certificate, Social Security card, driver's license, non-driver government-issued identification card, baptismal certificate, access device card, employee identification card, school identification card or other identifying information recorded by any other method, including, but not limited to, information stored on any computer, computer disc, computer printout, computer system, or part thereof, or by any other mechanical or electronic means.
- b. **Identifying information** - Any document, photographic, pictorial or computer image of another person, or any fact used to establish identity, including, but not limited to, a name, birth date, Social Security number, driver's license number, non-driver governmental identification number, telephone number, checking account number, savings account number, student identification number, employee or payroll number or electronic signature.

V. Procedures

A. First Responding Officers' Responsibilities

1. Officers responding to take a report concerning identity theft should:
 - a. Document all pertinent information on a UPPD Incident Report (UPPD-10). It is essential that officers collect clear and concise information from the complainant, including any names used, date of birth, social security numbers, date of discovery, dates of compromise, all accounts that have been affected including the account numbers, point of suspected compromise and any action that has already been taken by the complainant.
 - b. Important contact information and paperwork may have already been obtained for the compromised accounts and should be documented in the initial report.
 - c. The complainant should be informed to close any compromised accounts (if he/she has not done so already); notify the financial institutions and credit card companies affected, and to place a fraud alert with the various credit bureaus.

B. Assigned Detective's Responsibilities

1. The assigned detective investigating an initial report of an identity theft crime will:
 - a. Follow up with the complainant to obtain any additional information not documented in the original incident report.
 - b. Ensure that all compromised accounts have been closed.
 - c. Ensure that the complainant has notified the credit bureaus and has place a fraud alert with them. (Equifax, www.equifax.com , 800-525-6285; Experian, www.experian.com , 888-397-3742; and Trans Union, www.transunion.com , 800-680-7289).
 - d. Ensure that the complainant has received, or will receive, a copy of the initial incident report, and
 - e. Conduct an investigation into the complainant's report.
 - f. Ensure that the complainant obtains and completes an identity theft affidavit for each compromised or fraudulently opened account. The victim is required to prepare an affidavit stating they did not commit the fraud. In order to dispute a fraudulent account or transaction, a copy of this affidavit must be coupled with a copy of the police report, report summary, or report number, and sent to every creditor, business and debt collector through which a fraudulent account or transaction has occurred.
2. Coordination of investigation with other agencies

a. Should the investigation warrant, the assigned detective should coordinate the investigation of identity crimes with the following law enforcement entities:

- 1) Philadelphia Police Department
- 2) Pennsylvania State Police
- 3) Pennsylvania Office of the Attorney General
- 4) United States Postal Inspectors
- 5) Federal Trade Commission
- 6) Federal Bureau of Investigation
- 7) U.S. Department of Treasury

C. Records Unit Responsibilities

1. Victims of identity crimes are required to file a police report in order to dispute fraudulent transactions, correct compromised accounts, place fraud alerts with the credit bureaus and to obtain free copies of their credit reports to review. The Fair and Accurate Credit Transaction Act requires law enforcement to provide victims of identity theft with a copy of the police report. Records Unit staff will ensure that victims of identity theft requesting a copy of the initial police report be provided one in a timely manner.

D. Providing Public Information on Prevention of Identity Crime

1. From the Division of Public Safety's web page, members of the UPPD's service community may click on the following link to obtain information relative to identity crime:

<https://www.consumer.ftc.gov/features/feature-0014-identity-theft>

2. Detective Unit personnel will also provide informational materials to victims reporting identity crimes to the department.

E. Compliance

Violations of this directive, or portions thereof, may result in disciplinary action.

F. Officers Assigned to Other Agencies

Officers of this department assigned to or assisting other law enforcement agencies will be guided by this directive.

G. Application

This directive constitutes department policy, and is not intended to enlarge the employer's or employee's civil or criminal liability in any way. It shall not be construed as the creation of a higher legal standard of safety or care in an evidentiary sense with respect to third party claims insofar as the employer's or employee's legal duty as imposed by law. Violations of policy will only form the basis for departmental administrative sanctions. Violations of law will form the basis for civil and criminal sanctions in a recognized judicial setting.