ORLANDO POLICE DEPARTMENT POLICY AND PROCEDURE

1410.1, IDENTITY THEFT FILES MESSAGE KEY

EFFECTIVE:	12/10/2020
RESCINDS:	1410.0
DISTRIBUTION:	ALL EMPLOYEES
REVIEW RESPONSIBILITY:	PROPERTY SECTION COMMANDER
ACCREDITATION STANDARDS:	NONE
CHIEF OF POLICE:	ORLANDO ROLÓN

CONTENTS:

POLICY:

The Florida Department of Law Enforcement (FDLE) has programmed for new message keys related to the National Crime Information Center (NCIC) and the Florida Crime Information Center (FCIC) Identity Theft File. The Identity Theft File will serve as a means for law enforcement to "flag" stolen identities and identify the imposter when encountered by law enforcement.

PROCEDURES:

1. DEFINITIONS

IDENTITY THEFT FILE: Will serve as a means for law enforcement to "flag" stolen identities and identify the imposter when encountered by law enforcement.

2. REPORT REQUIRED

2.1 INITIAL INCIDENT REPORT

Identity Theft reports shall be taken when the victim becomes aware that his/her identity has been stolen (per F.S.S. 817.568) and reports the incident to law enforcement and the victim is:

a. A full time resident of the City of Orlando.
b. A victim who lives out of state who has identified an address in the city limits of Orlando where his/her identity was used.

3. REPORT PROCEDURES

3.1 PRIMARY OFFICERS RESPONSIBILITY

The primary officer will meet with the victim to complete an initial incident report. The initial officer shall also obtain pertinent information from the victim to create a victim profile that is entered into the FCIC/NCIC Identity Theft file if the following criteria are met.

a. Someone is using a means of identification of the victim (denoted in the Identity Theft and Assumption Deterrence Act of 1998 as any name or number that may be used alone or in conjunction with any other information, to identify a specific individual.
b. The identity is being used without the victim's permission.
c. The victim's identity is being used or intended to be used to commit an unlawful activity.

d. The victim must sign a consent waiver (Attachment A) prior to the information being entered into the Identity theft file. The attached waiver may be used independently or incorporated into a local complaint form.
e. Information on deceased persons may be entered into the file if it is deemed by the law enforcement agency that the victim's information has been stolen. No consent form (Attachment A) is required with the entry of deceased person information.

Information needed for the profile should contain information such as name, date of birth, social security number and the type of identity theft. Once the consent form is signed and completed it should be forwarded to Economic Crimes Supervisor within 48 hours.

3.2 ECONOMIC CRIMES SUPERVISOR

a. The Economic Crimes Sergeant will review the incident report and the consent form to determine that the general entry criteria have been met.
b. The report will then be assigned to a detective to be entered into the Identity Theft File.

3.3 ECONOMIC CRIMES UNIT RESPONSIBILITY

a. A detective shall be assigned to conduct the follow-up investigation when the report is received. The assigned detective is responsible for contacting the identity theft victim. The detective will request the victim provide a password to be entered into the Identity theft file. The detective shall advise the victim to retain this password to use during any potential future law enforcement encounters.
b. If the identity theft victim is deceased, the agency must enter the characters DECEASED as the password.
c. Detectives may also obtain a photo of the victim which may be entered into NCIC. The image may be entered as an additional form of identification for the victim. The detective must clearly specify in the message key that the photo is that of the victim/not the offender.

4.VALIDATION/RETENTION PERIOD

4.1 VALIDATION PERIOD

a. Identity Theft records will require validation thirty (30) days following entry, and annually thereafter.
b. OPD communications will validate all identity theft files each year. The validator runs each entry in teletype to see if it is still active. A list will be sent to the appropriate detective or sergeant who would verify if the file is still active or closed/cleared. After the detective/sergeant has made their determination, the list would be noted and returned to validations within the requested time frame.

4.2 RETENTION PERIOD

a. An identity theft record will remain active until the entering agency cancels it or until the Date of Purge (DOP) is equal to the current date. When the DOP is reached an administrative message will be sent to the originating agency.
b. Other exceptions to the record retention periods will occur in the event a serious error is detected in the record.
c. The maximum retention period for an identity theft record is five (5) years.

5. CANCELLATION OF IDENTITY THEFT RECORD

1. Cancellation of the identity theft record is restricted to the agency that entered the record. The record may be cancelled by the entering agency when:

a. The record is no longer valid
b. The victim withdraws consent
c. The complaint was found to be invalid
d. The date of purge is equal to the current date.

6. PROCEDURES FOR HANDLING A HIT

During an encounter by law enforcement, including routine traffic stops, a person's query into NCIC will automatically search the Identity Theft File and, if positive, generate a response to the inquiring agency. The officer will receive a response listing the victim profile, including the victim's password, thereby providing the officer with the information necessary to verify that the person encountered is the victim or that the person may be using a false identity.

The officer should be cognizant that the individual should not be arrested or detained based solely upon the information provided in the positive response from the Identity Theft File. The response should be considered along with additional information or circumstances surrounding the encounter before taking action.

ATTACHMENT A

IDENTITY THEFT FILE CONSENT DOCUMENT

By signing this document, I hereby provide the Orlando Police Department permission to enter my personal data into the Federal Bureau of Investigation's (FBI's) Identity Theft File. This information may include, but is not limited to, physical descriptors and identifying information including my name, date of birth, place of birth, Social Security number, the type of identity theft, and a password of my choosing for future identification verification purposes. I am also providing permission to enter my photograph and fingerprints into this file when that capability becomes available.

I understand that this information is being submitted as part of a criminal investigation of a crime of which I was a victim and will be available to entities having access to the FBI's National Crime Information Center (NCIC) files for any authorized purpose. I am providing this data voluntarily as a means to document my claim of identity theft and to obtain a unique password to be used for future identity verification purposes.

I understand that the FBI intends to remove this information from the NCIC active file no later than five years from the date of entry. I also understand that I may at any time submit a written request to the entering agency to have this information removed from the active file at an earlier date. I further understand that information removed from the active file will not thereafter be accessible via NCIC terminals, but it will be retained by the FBI as a record of the NCIC entry until such time as its deletion may be authorized by the National Archives and Records Administration.

I understand that this is a legally binding document reflecting my intent to have personal data entered into the FBI's Identity Theft File. I declare under penalty of perjury that the foregoing is true and correct. (See Title 28, United States Code [U.S.C.], Section 1746.)

I understand that it is my responsibility to notify the Orlando Police Department of any changes in my contact information, in order to complete the annual validation process. My failure to contact the Orlando Police Department of any contact changes may result in the removal of my information from my active identity theft file.

I understand that it is my responsibility to retain this password to use during any potential future law enforcement encounter.

_____ _____

SIGNATURE DATE

_____ _____

PRINTED NAME EMAIL ADRESS

_____

PASSWORD

The Privacy Act of 1974 (5 U.S.C. § 552a) requires that local, state, or federal agencies inform individuals whose Social Security number is being requested whether such disclosure is mandatory or voluntary, the basis of authority for such solicitation, and the uses which will be made of it. Accordingly, disclosure of your Social Security number is voluntary; it is being requested pursuant to 28 U.S.C. § 534 for the purposes described above. The Social Security number will be used as an identification tool; consequently, failure to provide the number may result in a reduced ability to make such identifications or provide future identity verifications.