

1 INTRODUCTION

1.1 BACKGROUND

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.

When an identity theft victim becomes aware that his/her identity has been stolen and reports the incident to law enforcement, the agency's handling of the identity theft case should parallel the criteria as outlined in this chapter.

1. The police officer should complete an incident report and collect pertinent information from the victim to create a victim profile that is entered into the Identity Theft File.
2. The agency enters the information only after the victim signs a consent waiver. The waiver states that the victim provides permission for the information to be entered in the Identity Theft File. It also acknowledges that the victim may withdraw the consent by providing a written request to the entering agency. At that time, the record will be canceled from the Identity Theft File. The profile should include information such as the victim's name, date of birth, Social Security number, and the type of identity theft.
3. In addition, a password is established either by the victim or the police officer and entered into the Identity Theft File. The password will identify the person as the victim and should be provided to the victim when the police report is filed. (The victim should retain the password to use during any potential future police encounters.)
4. Agencies may also enter a mug shot of the victim into NCIC. The mug shot may be used as an additional form of identification for the victim. When the mug shot is retrieved, it must clearly specify that the mug shot is that of the victim and not that of the offender.

During a subsequent 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 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 the officer takes action.

Information on deceased persons may also be entered into the Identity Theft File. If a police officer becomes aware of a deceased person's identity being stolen, that information can be entered into the file noting that the person is deceased.

1.2 CRITERIA FOR ENTRY

GENERAL CRITERIA

An entry in the Identity Theft File must be supported by an official complaint (electronic or hard copy) recorded by and on file at a law enforcement agency. Documentation for the identity theft complaint must meet the following criteria before an entry can be made into the Identity Theft File:

- 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).
- The identity of the victim is being used without the victim's permission.
- The victim's identity is being used or intended to be used to commit an unlawful activity.
- The victim must sign a consent waiver prior to the information being entered into the Identity Theft File. The following waiver may be used independently or incorporated into a state form.
- Information on deceased persons may be entered into the file if it is deemed by the police officer that the victim's information has been stolen. No consent form is required with the entry of deceased person information.
- If the identity of the thief is known and an arrest warrant has been issued, the agency should enter the victim information in the S/F Fields in the Wanted Person File.
- Only the agency that takes the identity theft complaint may make an NCIC identity theft entry. The only exception is that any criminal justice agency or regional dispatch center may act as a holder of the record for another agency that has no telecommunications equipment. When such an entry is made, the agency holding the record may place its own Originating Agency Identifier (ORI) in the ORI Field only when there is a written agreement between the two agencies that delineates the legal responsibility of each for the record.

IDENTITY THEFT FILE CONSENT DOCUMENT

By signing this document, I hereby provide the _____
(Insert local, state, or federal law enforcement agency name) 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 provided to me 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.)

SIGNATURE

DATE

PRINTED NAME

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 and _____ (add any applicable state authorization, if desired) 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.