

NCIC Identity Theft File Positive Response Example

The Password Field (PWD) is denoted in red.

WARNING - THE IDENTITY OF THE SUBJECT IDENTIFIED IN THIS RECORD HAS BEEN REPORTED STOLEN. REVIEW THE VICTIM PROFILE AND USE CAUTION IN VERIFYING THE IDENTITY OF THIS PERSON. THE PASSWORD INCLUDED IN THIS RESPONSE HAS BEEN ASSIGNED TO THE IDENTITY THEFT VICTIM. VERIFY THAT THE SUBJECT OF THE INQUIRY CAN CONFIRM THE PASSWORD.

MKE/IDENTITY THEFT

ORI/MD1012600 NAM/DOE, JOHN J SEX/M RAC/W
DOB/19830531 HGT/601 WGT/205 EYE/BRO HAIR/BRO
SKN/DRK SMT/SCR R HND FPC/121011C014159TTCI13
SOC/123456789 OCA/123ABC

MIS/IDENTITY HAS BEEN USED IN CREDIT CARD
FRAUD IN VARIOUS STATES

PWD/SNICKERDOODLE IDT/CFRD DOT/20050630

ORI IS ANY CITY PD MD 301-555-1212

NIC/J***** DTE/20050715 1400 EST

*****WARNING - STANDING ALONE, NCIC IDENTITY THEFT FILE INFORMATION DOES NOT FURNISH GROUNDS FOR THE SEARCH AND SEIZURE OF ANY INDIVIDUAL, VEHICLE, OR DWELLING.*****

For more detailed information on the Identity Theft File, consult the NCIC Operating Manual, contact your CJIS Systems Agency, or call the FBI's NCIC Training staff at 1-866-FBI-NCIC (324-6242).

Revised February 2007

U.S. Department of Justice
Federal Bureau of Investigation
Criminal Justice Information Services Division



The NCIC Identity Theft File



To Catch a Thief

This Document is Law Enforcement Sensitive

The Problem

Identity theft is viewed by many consumer privacy groups as the fastest-growing, white-collar crime in the nation. Recent Federal Trade Commission statistics indicate nearly 5 percent of the adult U.S. population has been a victim of identity theft with losses totalling more than \$5 billion. It can be devastating when someone uses another individual's personal identifying information to commit fraud. Armed with this information, an identity thief can open new bank or credit accounts posing as the victim, borrow funds or make purchases in the victim's name, or withdraw funds from the victim's existing accounts. Although far more prevalent, these financial crimes are not the only criminal uses of identity theft information -- it has even been used to evade detection in the commission of violent crimes.

The Identity Theft File

The National Crime Information Center (NCIC) Identity Theft File is a means for law enforcement to "flag" stolen identities and identify imposters when they are encountered.

Personal and biographic information entered into the Identity Theft File creates a "victim profile" that is made readily available to law enforcement during future encounters. A password is included in the file's victim profile and used for identification to law enforcement as the true identity. This password is created by the victim.

A password is included in the file's victim profile and used for identification to law enforcement as the true identity.

To qualify for entry into the NCIC Identity Theft File, the report taken by the law enforcement agency must meet the following three criteria:

Someone is using a means of identification for the victim;

The identity of the victim is being used without the victim's permission; and

The victim's identity is being used or intended to be used to commit an unlawful activity.

The victim must also sign a consent waiver, authorizing the law enforcement agency to make the NCIC Identity Theft File entry and provides the victim with instructions for requesting removal of the record from NCIC if desired.

The NCIC Identity Theft File can be searched independently, but it is also cross-checked with each inquiry of the Wanted Person File. Each hit includes the following instructions contained in the record caveat:

WARNING - THE IDENTITY OF THE SUBJECT IDENTIFIED IN THIS RECORD HAS BEEN REPORTED STOLEN. REVIEW THE VICTIM PROFILE AND USE CAUTION IN VERIFYING THE IDENTITY OF THIS PERSON. THE PASSWORD INCLUDED IN THIS RESPONSE HAS BEEN ASSIGNED TO THE IDENTITY THEFT VICTIM. VERIFY THAT THE SUBJECT OF INQUIRY CAN CONFIRM THE PASSWORD.

This caveat is followed by the victim profile information including physical descriptors and numeric identifiers to be used in addition to the password for identification.

Who Takes the Report?

Jurisdiction for investigating identity theft can sometimes be tricky. For example, an identity may be stolen in one place and used in another, while the victim lives in yet another location. But the entry criteria for the NCIC Identity Theft File does not address jurisdiction. Where programming exists, any law enforcement agency that takes an identity theft report meeting the criteria may enter the information into NCIC. Check with your state or federal CJIS Systems Agency for more information.

Investigative Assistance

Taking a police report not only benefits the victim, but the law enforcement agency as well. Section 609e of the Fair Credit Reporting Act allows the victim to send a copy of the police report, an affidavit, and a written request to the financial institution for the fraudulent transaction information and the company has 30 days to respond. The victim can even make the investigator their agent to receive the evidentiary information, removing the need for a subpoena or additional judicial process.