

Identity Theft is viewed by many consumer privacy groups as the fastest growing, white-collar crime in the Nation. In 2022, the Federal Trade Commission reported there were 1.1M identity theft reports made. Statistics indicate that 30 percent of individuals reporting identity theft were between the ages of 30 and 39. 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, which has been used to evade detection in the commission of violent crimes.

Investigative Assistance is a necessity. Filing 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 about the fraudulent transaction information. The company has 30 days to respond. The victim can make the investigator their agent to receive the evidence, thus removing the need for a subpoena or additional judicial process.

For Training regarding the NCIC Identity Theft File call 1-877-324-6242 or email: ncictraining@fbi.gov. For additional information regarding the Identity Theft File, consult the NCIC Operating Manual or contact your CJIS Systems Agency.

Additional Resources

TransUnion Group

1-800-680-7289

P.O. Box 6790
Fullerton, CA 92834

www.transunion.com

Experian (TRW)

1-888-397-3742

P.O. Box 9532
Allen, TX 75013

www.experian.com

Equifax

1-800-525-6285

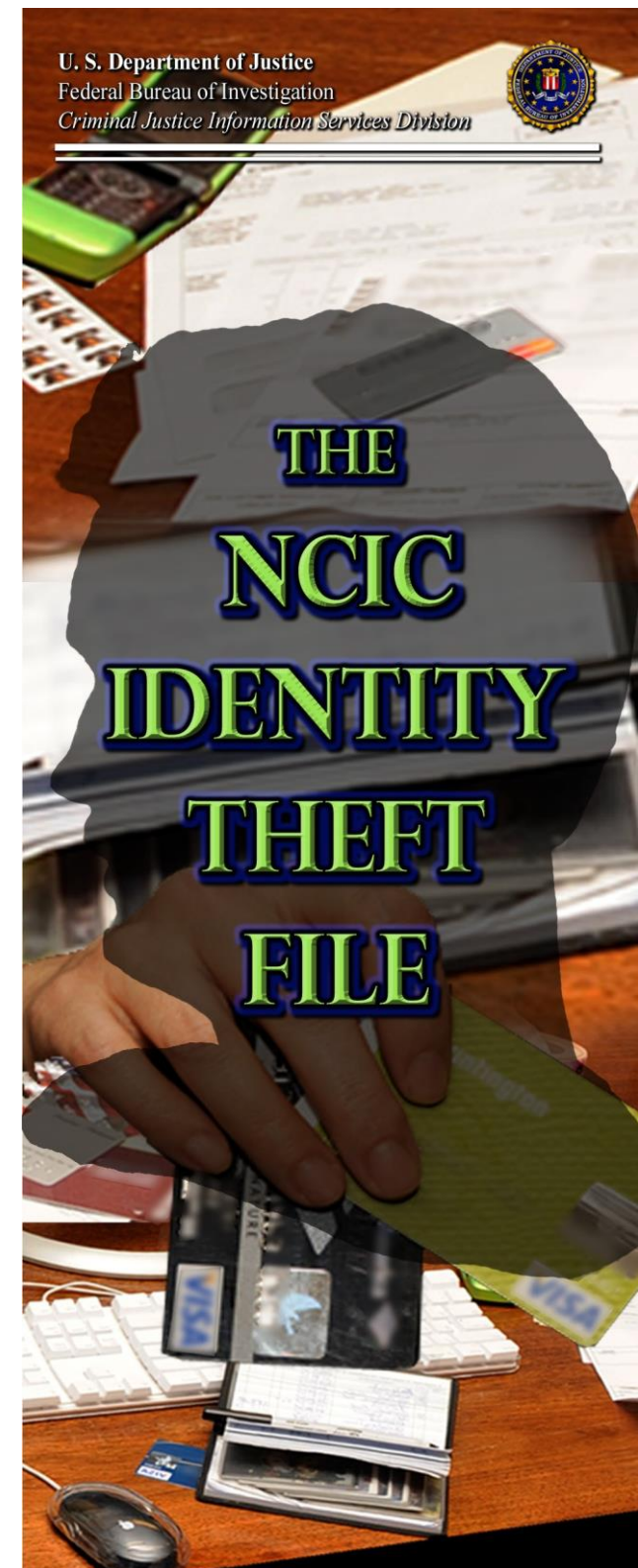
P.O. Box 74024
Atlanta, GA 30324

www.equifax.com

Federal Trade Commission

1-877-IDTHEFT

www.consumer.gov/idtheft



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 biographical information entered into the Identity Theft File creates a “victim profile” that is made readily available to law enforcement for future encounters. A victim-created password is included in the files and is 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:

- 1) Someone is using a means of identification of/from the victim.
- 2) The identity of the victim is being used without the victim’s permission.
- 3) 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 that authorizes 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 the NCIC if desired. Information on deceased persons may also be entered into the file if law enforcement deems that information has been stolen. In these cases, the word “DECEASED” is placed in the password field and no consent form is necessary.

Determining the Jurisdiction for investigating identity theft can sometimes be tricky. For example, a person’s identity may be stolen in one place and used in another while the victim lives in yet another location. The entry criteria for the NCIC Identity Theft File does not address jurisdiction issues. 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.

Top Identity Theft Crimes:

Below are the top 5 identity theft crimes of 2022:

1. Credit Card Fraud
2. Other Identity Theft
3. Bank Fraud
4. Loan or Lease Fraud
5. Employment or Tax Related Fraud

(Source: The Big View: All Sentinel Reports by Federal Trade Commission 09/2023)

If Your Identity is Stolen:

- Cancel all credit cards.
- Request a letter from the bank or credit institution confirming that a fraud has been committed against you and that you are not responsible for the ensuing debt.
- Close any of your accounts that have been compromised.
- File a police report in the jurisdiction where the theft occurred and obtain a copy to show creditors.
- Call the three national credit reporting organizations (Equifax, Experian, and TransUnion Group are listed on back of this brochure) to place a fraud alert on your name and social security number.
- Take notes and keep a record of conversations and make copies of correspondences. Retain this information indefinitely.
- Contact the Federal Trade Commission Identity Theft Hot Line at 877-ID-THEFT (877-438-4338) to file a complaint.
- Check your state’s Department of Motor Vehicles web site to determine if an unauthorized license has been issued in your name.
- After all related matters are corrected, request new credit reports to confirm that fact.

