Federal Deposit Insurance Corporation
550 17th Street NW, Washington, DC 20429

Identity Theft

FIL-100-99
October 29, 1999

TO: CHIEF EXECUTIVE OFFICER

SUBJECT: *Identity Theft and Assumption Deterrence Act of 1998*

The Federal Deposit Insurance Corporation (FDIC) has prepared guidance for bankers who suspect their customers may have been victims of identity theft. This crime was addressed with the October 30, 1998, enactment of the attached "Identity Theft and Assumption Deterrence Act of 1998" (Act), which in part amends 18 U.S.C. §1028 ("Fraud and related activity in connection with identification documents"). The following summarizes the provisions of the legislation and recommends certain actions that banks should take in responding to reports of identity theft.

Identity Theft and Assumption Deterrence Act of 1998

The Act (Pub. L. 105-318) addresses the problem of "identity theft"-the misappropriation of another person's identity (i.e., identifying information such as name, date of birth or Social Security number) for criminal purposes. The Act was needed because Section 1028 previously addressed only the fraudulent creation, use or transfer of identification *documents*, and not the theft or criminal use of the underlying personal *information*. The Act criminalizes fraud in connection with the unlawful theft and misuse of personal identifying information, regardless of whether the information appears or is used in documents. The Act also toughens the penalty provisions of Section 1028. With some exceptions, violations are generally subject to a fine and/or imprisonment of up to 15 years.

Section 3 of the Act amends 18 U.S.C. §1028 by, among other things, adding a new subsection to establish an offense by anyone who:

> "knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law."

"Means of identification" has been amended to include "any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual." Specific examples include an individual's name; Social Security number; date of birth; driver's license; unique biometric data, such as fingerprints or iris image; and unique electronic identification number and telecommunication identifying information or access device, such as an access code or personal identification number (PIN).

The definition of "document-making implement" has been modified to include computers and software specifically configured or primarily used for making identity documents. The Act is intended to cover a variety of individual identification information that may be developed in the future and used to commit identity theft crimes.

Section 5 of the Act directs the Federal Trade Commission (FTC), within one year, to establish a procedure to log in and acknowledge receipt of individuals' complaints, to provide educational materials to these individuals and to refer the complaints to the appropriate entities, including the three major national credit reporting bureaus and appropriate law enforcement agencies.

Customer Assistance Guidelines

If an institution suspects an illicit attempt has been made to obtain a customer's identity information, it should immediately report the matter to the proper authorities. In such circumstances, institutions are encouraged to file a Suspicious Activity Report (SAR), and to contact their primary federal banking regulator, the FTC, and the appropriate state agencies charged with enforcing laws against identity theft. In addition, institutions should directly contact the appropriate law enforcement agencies if the situation appears to require immediate attention.

Many victims of identity theft may need assistance in determining steps they should take to ameliorate the damage to their credit, reputation or other personal considerations. The bank should refer these individuals to the FTC, which can provide them with steps they can take to inform credit reporting agencies, credit issuers, law enforcement authorities and other agencies of the improper use of their identification information. The FTC also will provide the public with additional educational information recommending steps to be taken to prevent individuals from becoming victims of identity theft. Victims may call the FTC Consumer Response Center (1-877-FTC-HELP) or visit its Web site (www.consumer.gov/idtheft) for assistance in addressing their problems.

The FTC database of complaints will be a valuable source of information for identifying victims and perpetrators of possible criminal activity, and indicating whether the scope of the activity is purely local or covers a wide area. While the FTC is preparing the identity theft database, it will use its general consumer fraud database to log in complaints that may include instances of identity theft.

In addition to the federal identity theft statute, many states have enacted identity theft legislation or have such legislation pending. Consequently, victims of identity theft also may report instances of identity theft to state or local law enforcement agencies, which have authority to investigate these violations.

For further information, please contact the FDIC's Special Activities Section, 550 17th Street, NW, Room 6012, Washington, DC 20429. For your reference, all FDIC Financial Institution Letters published since January of 1995 may be found on the FDIC's Web site at www.fdic.gov/news/news/financial/index.html.

James L. Sexton
Director

Attachment: Public Law 105-318, Oct.30, 1998
PDF Format (122 Kb - PDF help or hard copy)

Distribution: FDIC-Supervised Banks (Commercial and Savings)

NOTE: Paper copies of FDIC financial institutions letters may be obtained through the FDIC's Public Information Center, 801 17th Street, NW, Room100, Washington, DC 20434 (800-276-6003 or (703) 562-2200).