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

IDENTITY THEFT AND PRETEXT CALLING

FIL-39-2001
May 9, 2001

TO: CHIEF EXECUTIVE OFFICER
SUBJECT: *Guidance on Identity Theft and Pretext Calling*

The Federal Deposit Insurance Corporation (FDIC) is issuing the attached "Guidance on Identity Theft and Pretext Calling" to inform banks about developments in these two areas of consumer bank fraud. The other federal banking agencies are issuing similar guidance on this matter. Each agency's guidance is consistent with one another. The guidance:

- summarizes federal laws that pertain to identity theft and pretext calling;
- discusses measures institutions can take to protect customer information;
- informs institutions how they should report suspected criminal activity;
- highlights the importance of consumer education to prevent fraud and assist victims of fraud; and
- provides references for additional assistance and previous FDIC publications regarding or relating to identity theft and pretext calling.

This guidance is in response to provisions in the Gramm-Leach-Bliley Act (GLBA) that direct the FDIC and other federal banking agencies to review their regulations and guidelines to ensure that financial institutions have policies, procedures and controls in place to prevent the unauthorized disclosure of customer financial information and to deter and detect fraudulent access to such information. Consistent with section 525 of the GLBA (15 U.S.C. 6825), the FDIC has developed the attached guidance to address how banks should protect customer information against identity theft. The guidance supplements guidelines on customer information security issued on February 1 pursuant to section 501(b) of the GLBA. The guidelines take effect on July 1, 2001.

For more information, please contact Carol A. Mesheske, Chief, Special Activities Section, in the Division of Supervision, at (202) 898-6750 or Marc J. Goldstrom, Counsel in the Legal Division, at (202) 898-8807.

Michael J. Zamorski
Acting Director

Attachment: Guidance On Identity Theft And Pretext Calling

Distribution: FDIC-Supervised Banks (Commercial and Savings)

NOTE: Paper copies of FDIC financial institution letters may be obtained through the FDIC's Public Information Center, 801 17th Street, NW, Room 100, Washington, DC 20434 (800-276-6003 or 202-416-6940).

GUIDANCE ON IDENTITY THEFT AND PRETEXT CALLING

The Gramm-Leach-Bliley Act (GLBA) directs the Federal Deposit Insurance Corporation (FDIC) and other federal banking agencies to review their regulations and guidelines to ensure that financial institutions have policies, procedures and controls in place to prevent the unauthorized disclosure of customer financial information and to deter and detect fraudulent access to such information. Consistent with section 525 of the GLBA (15 U.S.C. 6825), the FDIC has developed the following guidance to address how banks should protect customer information against identity theft. Guidance is also included on completing Suspicious Activity Reports (SARs) to report offenses associated with identity theft and pretext calling, i.e., posing as a customer or someone authorized to have customer information in order to obtain confidential customer data.

Several federal criminal statutes address illegal conduct associated with identity theft and pretext calling. These include:

- The Federal Criminal Code (18 U.S.C. 1028), which makes it a crime to knowingly use, without lawful authority, a means of identification (such as an individual's Social Security number or date of birth) of another person with the intent to commit a crime.
- Sections 521 and 523 of the GLBA (15 U.S.C.6821, 6823), which make it a crime to obtain customer information by means of false or fraudulent statements to an officer, employee, agent or customer of a financial institution.
- Sections 521 and 523 of the GLBA, which also make it a crime to request a third party to obtain customer information from a bank or other financial institution, if the requester knows the information will be obtained through fraudulent methods. (This generally means a bank using customer information obtained by pretext calling could be subject to criminal sanctions if the institution knew how the information was obtained.)

Institutions are reminded of guidance recently issued by the FDIC and the other banking agencies concerning the safeguards financial institutions can put into place to help prevent the problems caused by pretext calling.

Protecting Customer Information

Banks should take various steps to safeguard customer information and reduce the risk of loss from identity theft. These include: (1) establishing procedures to verify the identity of individuals applying for financial products; (2) establishing procedures to prevent fraudulent activities related to customer information; and (3) maintaining a customer information security program.

1. Verification Procedures. Verification procedures for new accounts should include, as appropriate, steps to ensure the accuracy and veracity of application information. These could involve using independent sources to confirm information submitted by a customer; calling a customer to confirm the customer has opened a credit card or checking account; using an independently verified telephone number; or verifying information through an employer identified on an application form. A financial institution can also independently verify the zip code and telephone area code provided on an application are from the same geographical area.

2. Fraud Prevention. To prevent fraudulent address changes, banks should verify customer information before executing an address change and send a confirmation of the address change to both the new address and the address of record. If a bank gets a request for a new credit card or new checks in conjunction with a change of address notification, it should verify the request with the customer.

When opening a new account, a bank should, where possible, check to ensure information provided on an application has not previously been associated with fraudulent activity. For example, if a bank

uses a consumer report to process a new account application and the report is issued with a fraud alert, the bank's system for credit approval should flag the application and ensure the individual is contacted before it is processed. In addition, fraud alerts should be shared across the bank's various lines of business.

3. Information Security. On February 1, 2001, the federal banking agencies issued guidance on the security of customer information ("Interagency Guidelines for the Safeguarding of Customer Information by Financial Institutions," 66 Fed. Reg. 8616 (February 1, 2001) (the "Guidelines")).

The Guidelines require financial institutions to implement a comprehensive information security program that includes appropriate administrative, technical, and physical safeguards for customer information. To prevent pretext callers from using pieces of personal information to impersonate account holders in order to gain access to their account information, the Guidelines require banks to establish written policies and procedures to control access to customer information.

Other measures that may reduce the incidence of pretext calling include limiting the circumstances under which customer information may be disclosed by telephone. For example, a bank may not permit employees to release information over the telephone unless the requesting individual provides a proper authorization code (other than a commonly used identifier). Banks can also use Caller ID or a request for a call back number as tools to verify the authenticity of a request.

Banks should train employees to recognize and report possible indicators of attempted pretext calling. They should also implement testing to determine the effectiveness of controls designed to thwart pretext callers, and may consider using independent staff or third parties to conduct unscheduled pretext phone calls to various departments.

Reporting Suspected Identity Theft and Pretext Calling

Banks are required by regulation to report all known or suspected criminal violations to law enforcement and regulatory agencies on SARs. Criminal activity related to identity theft or pretext calling has historically manifested itself as credit or debit card fraud, loan or mortgage fraud, or false statements to the institution, among other things.

As a means of better identifying and tracking known or suspected criminal violations related to identity theft and pretext calling, a bank should, in addition to reporting the underlying fraud (such as credit card or loan fraud) on a SAR, also indicate within the SAR that such a known or suspected violation is the result of identity theft or pretext calling. Specifically, when identity theft or pretext calling is believed to be the underlying cause of the known or suspected criminal activity, the reporting institution should, consistent with the existing SAR instructions, complete a SAR in the following manner:

- In Part III, Box 35, of the SAR, check all appropriate boxes that indicate the type of known or suspected violation being reported and, **in addition**, in the "Other" category, write in "identity theft" or "pretext calling," as appropriate.
- In Part V of the SAR, in the space provided for the narrative explanation of what is being reported, include the grounds for suspecting identity theft or pretext calling in addition to the other violation being reported.
- In the event the only known or suspected criminal violation detected is the identity theft or pretext calling, then write in "identity theft" or "pretext calling," as appropriate, in the "Other" category in Part III, Box 35, and provide a description of the activity in Part V of the SAR.

Consumer Education

In June 2000, the FDIC issued the Federal Trade Commission (FTC) consumer education pamphlet entitled "ID Theft: When Bad Things Happen To Your Good Name" and published an article on identity theft in the Summer 2000 issue of FDIC Consumer News. The Appendix provides a complete listing of FDIC publications relating to these topics and instructions on how to obtain them. Also, the FDIC's Web site, www.fdic.gov, is periodically updated to contain the latest information on these topics. Another excellent source of information for consumers is the U.S. government's central Web site for

information about identity theft maintained by the FTC, www.consumer.gov/idtheft. Banks may wish to make available to their customers information about how to prevent identity theft and necessary steps to take in the event a customer becomes a victim of identity theft.

Banks should assist their customers who are victims of identity theft and fraud by having trained personnel to respond to customer inquiries; by determining whether an account should be closed immediately after a report of unauthorized use; and by prompt issuance of new checks or new credit, debit or ATM cards. If a customer has multiple accounts with the institution, it should assess whether any other account has been the subject of potential fraud.

APPENDIX: LIST OF AGENCY ISSUANCES REGARDING INFORMATION SECURITY

Below is a list of FDIC publications regarding or related to identity theft and pretext calling. These documents may be accessed at the FDIC's Web site (www.fdic.gov) or (except as indicated below) in the FDIC Public Information Center, Room 100, 801 17th Street, NW, Washington DC 20429. Banks are encouraged to familiarize themselves with the contents of each issuance.

- Interagency Guidelines Establishing Standards for Safeguarding Customer Information, 66 Fed. Reg. 8616, 8638 (February 1, 2001), to be codified at 12 C.F.R. Part 364, App. B.
- "When a Criminal's Cover Is Your Identity," FDIC Consumer News, Summer 2000 (only available through the FDIC's Web site).
- "ID Theft: When Bad Things Happen To Your Good Name" (issued June 14, 2000) (only available through the FDIC's Web site). Banks interested in reproducing this brochure for their customers may obtain a PDF file at www.ftc.gov/bcp/conline/pubs/credit/idtheft.pdf.
- Identity Theft and Assumption Deterrence Act of 1998, Financial Institution Letter 100-99 (October 29, 1999).
- Pretext Phone Calling, Financial Institution Letter 98-98 (September 2, 1998).