FEDERAL RESERVE BANK
OF DALLAS

DALLAS, TEXAS
75265-5906

May 11, 2001

Notice 01-40

TO: The Chief Executive Officer of each
financial institution and others concerned
in the Eleventh Federal Reserve District

SUBJECT

Supervisory Guidance Regarding Protecting Customer Information Against Identity Theft

DETAILS

The Board of Governors of the Federal Reserve System has issued supervisory guidance addressing how banking organizations should protect customer information against identity theft. Recommended steps to safeguard information include establishing procedures to verify the identity of individuals applying for financial products, preventing fraudulent address changes, and blocking pretext callers from using pieces of personal information to impersonate account holders and gain access to account information.

Guidance is also provided on completing Suspicious Activity Reports that are filed by banking organizations with law enforcement agencies reporting offenses associated with identity theft and pretext calling.

The guidance is consistent with the Gramm-Leach-Bliley Act, which directs the Board and other federal agencies 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. Previously issued interagency guidance regarding the safeguarding of customer information is available on the Board's web site at **http://www.federalreserve.gov/boarddocs/press/boardacts/2001/20010117/default.htm**.

ATTACHMENT

A copy of the Board's supervisory letter (SR 01-11) dated April 26, 2001, is attached. The Board's supervisory guidance was previously issued with **Notice 01-22**, dated March 5, 2001.

MORE INFORMATION

For more information, please contact Gary Krumm, Banking Supervision Department, at (214) 922-6218. For additional copies of this Bank's notice, contact the Public Affairs Department at (214) 922-5254 or access our web site at **http://www.dallasfed.org/banking/notices/index.html.**

BOARD OF GOVERNORS
OF THE
FEDERAL RESERVE SYSTEM

WASHINGTON, D. C. 20551

DIVISION OF BANKING
SUPERVISION AND REGULATION

SR 01-11 (SUP)
April 26, 2001

TO THE OFFICER IN CHARGE OF SUPERVISION AND SUPERVISORY STAFF AT EACH FEDERAL RESERVE BANK AND TO EACH DOMESTIC AND FOREIGN BANKING ORGANIZATION SUPERVISED BY THE FEDERAL RESERVE

SUBJECT: Identity Theft and Pretext Calling

Purpose

The Gramm-Leach-Bliley Act directs the Board and other federal agencies 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 Gramm-Leach-Bliley Act (15 U.S.C. 6825), this SR letter addresses how state member banks and other banking organizations supervised by the Federal Reserve that provide products or services to the public or that maintain customer account information should protect customer information against identity theft. Guidance is also provided on completing Suspicious Activity Reports ("SARs") that report offenses associated with identity theft and pretext calling. In addition, banking organizations are reminded that guidance was recently issued by the Board and the other banking agencies concerning the safeguards that institutions can put into place to ensure the security of customer information.

Background

The fraudulent use of an individual's personal identifying information, such as social security number, date of birth, or bank account number, to commit a financial crime like credit card, check, loan or mortgage fraud - - which is commonly referred to as "identity theft" - - is a growing problem. One way that wrongdoers improperly obtain personal information of bank customers so as to be able to commit identity theft is by contacting a bank, posing as a customer or someone authorized to have the customer's information, and through the use of trickery and deceit, convincing an employee of the bank to release customer identifying information. This practice is referred to as "pretext calling."

There are several federal criminal statutes that address illegal conduct associated with identity theft and pretext calling. These include:

- Section 1028 of the Federal Criminal Code (18 U.S.C. 1028) 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.

- Section 523 of the Gramm-Leach-Bliley Act (15 U.S.C. 6828) makes it a crime to obtain customer information of a financial institution by means of false or fraudulent statements to an officer, employee, agent or customer of a financial institution.

- Section 523 of the Gramm-Leach-Bliley Act also makes it a crime to request another person to obtain customer information of a financial institution, if the requester knows that the information will be obtained by making a false or fraudulent statement. This generally means that a banking organization requesting customer information that is obtained by pretext calling could be subject to criminal sanctions if the institution knew how the information would be obtained.

Protecting Customer Information

Banking organizations can 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 that the customer has opened a credit card or checking account; or verifying information through an employer identified on an application form. A financial institution can also independently verify that 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, banking organizations 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 an organization receives 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 banking organization should, where possible, check to ensure that information provided on an application has not previously been associated with fraudulent activity. For example, if a banking organization uses a consumer report to process a new account application and the report is issued with a fraud alert, the banking organization's system for credit approval should flag the application and ensure that the individual is contacted before it is processed. In addition, fraud alerts should be shared across the organization's various lines of business.

3. **Information Security.** In early 2001, the Board and the other federal banking agencies issued *Interagency Guidelines Establishing Standards for Safeguarding Customer Information* , a copy of which is attached.[1] The Guidelines require banking organizations to establish and 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 and other financial institutions 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 banking organization 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). Banking organizations can also use caller identification technology or a request for a call back number as tools to verify the authenticity of a request.

Banking organizations 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

Current regulations require state member banks and other banking organizations supervised by the Federal Reserve to report all known or suspected criminal violations to law enforcement and the Board 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 banking organization 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 and Assistance

Banking organizations should provide their customers with information about how to prevent identity theft and necessary steps to take in the event a customer becomes a victim of identity theft. An excellent source of information for consumers is the Federal Trade Commission's website at http://www.consumer.gov/idtheft/.

Banking organizations should also 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.

Reserve Banks are asked to send a copy of this letter to regulated institutions in their districts and to their supervisory staff. Questions concerning identity theft, pretext calling, and suspicious activity reporting should be directed to Richard A. Small, Deputy Associate Director, at (202) 452-5235. Questions concerning information security should be directed to Heidi Richards, Assistant Director, at (202) 452-2598.

Richard Spillenkothen
Director