REGULATORY ALERT

NATIONAL CREDIT UNION ADMINISTRATION
1775 Duke Street, Alexandria, VA 22134

DATE: **February 1999** **NO.: 99-RA-3**

TO: **ALL FEDERALLY INSURED CREDIT UNIONS:**

SUBJ: **Pretext Phone Calling by Account Information Brokers**

The Office of the Comptroller of the Currency, the Federal Deposit Insurance Corporation, the Office of Thrift Supervision, the Federal Reserve Board, the Secret Service, the Federal Bureau of Investigation, the Internal Revenue Service, and the Postal Inspection Service recently issued an advisory letter to banks warning of a growing threat to the confidentiality of customer account information.

The practice of "pretext phone calling" involves illicit gathering of confidential information by individuals purporting to be a particular customer. This information is then used for fraudulent or illicit purposes. We believe credit unions may also be prime targets. Unauthorized access to sensitive customer account information also may occur through other avenues.

Credit unions have a responsibility to their members to ensure that their members' account information is not improperly disclosed. The enclosed advisory letter provides guidance for establishing policies, procedures, and an internal control environment that would preclude the dissemination of customer or member information to unauthorized individuals.

Sincerely,

/S/
Norman E. D'Amours
Chairman

Enclosure

FDIC

Federal Deposit Insurance Corporation
Washington, DC 20429

Office of the Director
Division of Supervision

FIL-98-98
September 2, 1998

SPECIAL ALERT

TO: CHIEF EXECUTIVE OFFICER

SUBJECT: Pretext Phone Calling

This Financial Institution Letter alerts bankers to the practice of "pretext phone calling" which is a means of gaining access to customers' confidential account information by organizations and individuals who call themselves "account information brokers." This letter is intended to enhance institutions' awareness regarding the confidentiality and sensitivity of customer information generally, and identify some appropriate measures for the safeguarding of such information.

This advisory was jointly prepared by the Federal Deposit Insurance Corporation (FDIC), the Office of the Comptroller of the Currency, the Office of Thrift Supervision, the Federal Reserve Board, the Federal Bureau of Investigation, the Secret Service, the Internal Revenue Service, and the Postal Inspection Service.

BACKGROUND

There is a tremendous demand for information about individuals' and businesses' bank accounts. In recent years, this rising demand for account information has led to an increase in the number of organizations known as "account information brokers." These "brokers" gather confidential financial information, including specific account numbers and balances, from various public and nonpublic sources. The brokers then sell this information to anyone who is willing to pay for it. Their clients include lawyers, debt collection services, and private investigators, who may use account information in civil lawsuits and other court proceedings, or identity thieves who may use account information to engage in check and credit card fraud, and other criminal acts.

Unscrupulous account information brokers are obtaining customers' account information from insured financial institutions through a practice known as "pretext phone calling" or "social

engineering." Brokers who engage in this practice call institutions and use surreptitious or fraudulent means to try to induce employees into providing a customer's account information. For example, a broker may pose as a customer who has misplaced his or her account number, and may repeatedly call the institution until the broker finds an employee who is willing to divulge confidential account information. The broker may use information about the customer, such as the customer's social security number, that has been obtained from other sources, to convince the employee that the caller is legitimate. While there are no reliable estimates as to the extent of this practice, there is concern among the federal banking and law enforcement agencies that it is becoming increasingly prevalent.

The use of surreptitious or fraudulent means to obtain a customer's account information may violate state and federal laws prohibiting unfair and/or deceptive practices. It also may violate federal wire fraud laws. In addition, institutions that disclose customers' account information may be violating state privacy laws, such as those that prohibit the release of a customer's financial records without having first obtained the customer's permission.

RECOMMENDED ACTION

Institutions have an obligation to their customers to ensure that their customers' account information is not improperly disclosed. Authorizing employees to use their own discretion to determine whether to disclose confidential information over the telephone can result in inconsistent practice and expose the institution and its customers to the risk of an inappropriate or unauthorized release of information. To avoid this risk, institutions are encouraged to develop policies and procedures for addressing customers' financial privacy**,** and should, at a minimum, establish clear guidelines for dissemination of customer account information. These guidelines should set forth precisely the types of information and the circumstances under which an employee is allowed to disseminate such information over the telephone. Employee training should ensure that all employees are aware of their responsibility to safeguard customer financial information, and also should educate employees about the tactics used by information brokers to surreptitiously or fraudulently obtain confidential customer information.

Institutions should have strong controls in place to ensure against the unauthorized disclosure of customer information. For example, they could consider adopting a policy that prohibits the release of information over the telephone unless the proper authorization code is provided. The authorization code would be used in the same manner as a personal identification number (PIN) for transacting business by automated teller machines, or credit, debit, or stored-value cards. The authorization code should not be associated with other commonly used numbers or identifiers, such as social security numbers, savings, checking, loan or other financial account numbers, PINS, or the customer's mother's maiden name. In addition, the authorization code should be unique to, and readily changed by, the authorized account holder. Finally, to increase effectiveness, the authorization code should be used in conjunction with other customer and account identifiers.

Another means of preventing unauthorized disclosures might be to use a caller identification service or require employees who receive calls requesting account information to ask the caller for the number from which he or she is calling. If the number differs from that in the customer's account records, it may be an indication that the request is not a legitimate one, and the employee should not disclose the requested account information without taking further steps to verify that the customer made the request.

The institution's security or internal audit department should consider conducting (or using third parties to conduct) unscheduled pretext phone calls to various departments to evaluate the institution's susceptibility to unauthorized disclosures of customer information. Any weaknesses detected should be addressed through the adoption of enhanced training, procedures, and controls.

While this advisory primarily concerns the unauthorized access to customer account information through pretext phone calling, unauthorized access to sensitive account information may occur through other means as well, including burglary, illegal or unauthorized access to the institution's computer systems, and bribing employees with access to personal account information. Institutions should have effective procedures and controls in place to limit access to confidential information on a need to know basis, and to prevent unauthorized access to customer information through these and other means, including ensuring that all sensitive documents are properly disposed of and that the institution's physical premises and computer systems are secure. Institutions also must properly train employees to understand the importance of protecting personal account information against improper disclosure. The federal banking agencies will continue to monitor institutions' efforts to safeguard sensitive account information.

Institutions that suspect an illicit attempt to obtain a customer's confidential information 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 Federal Trade Commission, and the appropriate state agencies charged with enforcing laws against unfair or deceptive practices. In addition, institutions should directly contact appropriate law enforcement agencies if a fraud requiring immediate attention is suspected.

Inquiries may be directed to the FDIC's Special Activities Section, 550 17thStreet, NW, Room F-6012, Washington, DC 20429.

Nicholas J. Ketcha Jr.
Director

Distribution: FDIC-Supervised Banks (Commercial and Savings)