NCUA LETTER TO CREDIT UNIONS

NATIONAL CREDIT UNION ADMINISTRATION
1775 Duke Street, Alexandria, VA

DATE: **September 2001** **LETTER NO.: 01-CU-09**

TO: **Federally Insured Credit Unions**

SUBJ: **Identity Theft and Pretext Calling**

ENCL: **(1) Guidance on Identity Theft and Pretext Calling**
(2) Appendix
(3) Identity Theft Brochure

The Gramm-Leach-Bliley Act (GLBA) requires the NCUA to provide guidance to credit unions concerning the unauthorized disclosure of financial information. In response to this requirement, the NCUA has developed the enclosed, *Guidance on Identity Theft and Pretext Calling*, to address how credit unions should protect member information against these two areas of consumer fraud. The Guidance:

- summarizes federal laws that pertain to identity theft and pretext calling;
- discusses measures credit unions can take to protect member information;
- informs credit unions 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 NCUA publications regarding or relating to identity theft and pretext calling.

Also enclosed you will find NCUA's member pamphlet, *How to Avoid Becoming a Victim of Identity Theft*. This pamphlet is available for download from NCUA's website (www.ncua.gov).

If, after reviewing the enclosed documents, you have any questions or concerns, please contact your NCUA Regional Office or State Supervisory Authority.

Sincerely,

/s/

Dennis Dollar
Chairman

Enclosures

GUIDANCE ON IDENTITY THEFT AND PRETEXT CALLING

The Gramm-Leach-Bliley Act (GLBA) directs the NCUA and the other agencies for federal financial institutions 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 member 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 NCUA has developed the following guidance to address how credit unions should protect member 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 member or someone authorized to have member information in order to obtain confidential member 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 member information by means of false or fraudulent statements to an officer, employee, agent, or member of a financial institution.

- Sections 521 and 523 of the GLBA, which also make it a crime to request a third party to obtain member information from a credit union or other financial institution, if the requester knows the information will be obtained through fraudulent methods. (This generally means a credit union using member information obtained by pretext calling could be subject to criminal sanctions if the credit union knew how the information was obtained.)

Protecting Member Information

Credit unions should take various steps to safeguard member 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 member information; and (3) maintaining a member 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 member; calling a member to confirm the member 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 credit union 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, credit unions should verify member 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 credit union 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 member.

When opening a new account, a credit union should, where possible, check to ensure information provided on an application has not previously been associated with fraudulent activity. For example, if a credit union uses a consumer report to process a new account application and the report is issued with a fraud alert, the credit union'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 credit union's various lines of business.

3. Information Security. In February 2001, the NCUA revised the NCUA Rules and Regulations, Part 748 and issued guidance (Guidelines for the Safeguarding Member Information) on the security of member information.

The regulation requires credit unions to implement a comprehensive information security program that includes appropriate administrative, technical, and physical safeguards for member 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 regulation requires credit unions to establish written policies and procedures to control access to member information.

Other measures that may reduce the incidence of pretext calling include limiting the circumstances under which member information may be disclosed by telephone. For example, a credit union 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). Credit unions can also use Caller ID or a request for a call-back number as tools to verify the authenticity of a request.

Credit unions 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

Credit unions are required by regulation to report all known or suspected criminal violations to law enforcement and regulatory agencies on Suspicious Activity Reports (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 credit union 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 credit union 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

The Federal Trade Commission (FTC) developed a consumer education pamphlet entitled "ID Theft: When Bad Things Happen To Your Good Name" which credit unions may use to provide information and assistance to their members. The Appendix to this Letter provides a complete listing of NCUA publications relating to these topics and instructions on how to obtain them. Also, the NCUA's Web site, www.ncua.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. Credit unions may wish to make available to their members information about how to prevent identity theft and necessary steps to take in the event a member becomes a victim of identity theft.

Credit unions should assist their members who are victims of identity theft and fraud by having trained personnel to respond to member 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 member has multiple accounts with the credit union, the credit union 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 NCUA publications regarding, or related to, identity theft and pretext calling. These documents may be accessed at the NCUA Web site (www.ncua.gov) or ordered from NCUA's Publications Office, 1775 Duke Street, Alexandria, VA 22314-3428 (703-518-6340). Credit unions are encouraged to familiarize themselves with the contents of each issuance.

- NCUA Rules and Regulations, Part 748 and Appendix.
- NCUA Rules and Regulations, Part 716 Privacy of Consumer Financial Information and Appendix.
- Letter to Credit Unions #01-CU-02 Privacy of Consumer Financial Information.
- Letter to Credit Unions #00-CU-02 Identity Theft Prevention.
- Letter to Credit Unions #99-CU-05 Interagency Statement on Retail On-line PC Banking.
- Regulatory Alert #99-RA-3 Pretext Phone Calling by Account Information Brokers.

Other Relevant Publications

"Identity Theft: What to Do if it Happens to You" Available at: www.pirg.org.
"Identity Theft: When Bad Things Happen to Your Good Name" Available at: www.consumer.gov/idtheft.

Websites That Provide Further Guidance and Information

Federal Trade Commission - www.consumer.gov/idtheft and www.ftc.gov
U.S. PIRG and CALPIRG - www.pirg.org
Privacy Rights Clearing House – www.privacyrights.org
Identity Theft Survival Kit – www.identitytheft.org
Better Business Bureau – www.bbbonline.org