NCUA LETTER TO CREDIT UNIONS

NATIONAL CREDIT UNION ADMINISTRATION
1775 Duke Street
Alexandria, VA 22314

DATE: January 13, 1997 LETTER NO. 97-CU-1

SUBJECT: Automated Response System Controls

This is to advise you of an internal control weakness in some automated response systems (e.g., audio response systems, home banking systems, etc.) that may affect a number of credit unions. Some automated response systems allow a user to access a member's account using the member's account number and an assigned personal identification number (PIN) which is the last four digits of the member's social security number. Both of these numbers are often easily obtained and can be used to gain access to a member's deposits.

For example, in several states an individual's drivers license number is his or her social security number. In this case, merchants receiving share drafts, in addition to credit union employees, have the information needed to access the member's credit union account. Additionally, with a copy of a member's check, duplicate checks can be made. Then, via audio response, unauthorized persons can transfer funds from savings to checking, and subsequently write checks with a fake driver's license as identification.

Compounding this problem is the failure on the part of some credit unions to establish limits for funds withdrawn using automated response systems. When no limit is set, the information system defaults to the system's limit which is often $99,999.

In some instances, the last four digits of the member's social security number are the PIN temporarily assigned to the member, allowing him or her to initially log on to the automated response system. Sometimes, but not always, the member receives instructions stating that the member should change the PIN to a unique number during the first log on. While this control is helpful, it does not mandate the change of the PIN, and the member is able to continue to use the social security number if he or she chooses not to change it. Additionally, some credit unions do not instruct members who are new users of automated response systems how and when to change their PINs.

Credit unions are encouraged to institute the following internal controls to protect the accounts and sensitive information of members who use automated response systems:

- Ideally, credit unions' information systems will protect sensitive member account access and information by assigning randomly-generated PINs to members who use automated response systems.

- If assigning randomly-generated PINs is impossible, the credit union should program its information system to allow the member to access his or her account using the social security PIN only once. If possible, the credit union should require members to change their PINs during their initial access. If the credit union's automated response processing system will not mandate changing the PINs during initial access, the credit union must warn members of the inherent risks of not making the change.

- Additionally, credit unions should establish dollar limits, both a transaction limit and an aggregate daily limit, on the amounts their members can access using automated response systems. These limits can vary from one credit union to another, but they should be reasonable for the credit union's membership. NCUA further suggests that credit unions consider establishing daily limits on the number of transactions that members can perform.

We have instructed our examiners to review, in future examinations, the internal controls surrounding automated response systems, paying particular attention to those weaknesses described herein.

/S/

Norman E. D'Amours
Chairman

(Letter No. 97-CU-1 and cover memo sent via ms-mail to all RDs, with cc to OED, GC, OA, OTIS, and CDCU 1/17/97.)

(Letter No. 97-CU-1 sent via ms-mail to all NCUA staff 1/22/97.)