National Credit Union Administration

CORPORATE CREDIT UNION GUIDANCE LETTER

No. 2010-01 DATE: July 8, 2010

SUBJ: Confidentiality and Protection of Sensitive Data

TO: The Corporate Credit Union Addressed:

The purpose of this letter is to inform corporate credit unions of the security measures in place to ensure the confidentiality and protection of sensitive data about or acquired from corporate credit unions or any other party external to NCUA. Sensitive data includes both electronic and hardcopy materials. NCUA has specific policies and procedures on staff's custodial responsibilities for safe guarding and destroying documents and information. Our staff is trained on these policies and procedures to secure NCUA issued laptops, confidential information residing on these laptops, as well as hardcopy documents. It is our goal to prevent disclosure of sensitive information to unauthorized parties.

For examination and supervision purposes, Office of Corporate Credit Union (OCCU) examiners and office staff have the authority and need to access and store data about your corporate credit union. To ensure control and confidentiality of your corporate credit union's data, we adhere to the following procedures:

- Examiners obtain data directly from your corporate credit union. They do not obtain data directly from your outside vendor without your corporate credit union's knowledge and authorization.
- Examiners will never access your corporate credit union's computer system and extract data without the knowledge and permission of your corporate credit union's staff.
- Examiner computers are password protected. Examiners have been instructed to lock their computers when they leave their work area. To access the computer after shutting down or hibernation, the examiner must enter a user name and corresponding password.
- Examiner computer hard drives and portable storage devices are encrypted and password protected. Unique passwords are needed to access the computer hard drives and portable storage devices.
- After each examination, examiners destroy unnecessary data. NCUA examination reports may contain some sensitive data obtained from your corporate credit union, but are NCUA property and considered confidential, privileged, and exempt from public disclosure.

- Obsolete hard drives of laptops and servers are properly disposed according to the National Institute of Standards and Technology Publication 800-88 "Guidelines for Media Sanitization."
- Document security control logs are used to track and control documentation if taken off corporate credit union premises.

NCUA also requires staff to encrypt or use secure E-mail for any sensitive information being exchanged via E-mail and/or with electronic attachments. Corporate credit unions' sending sensitive information to NCUA are encouraged to password protect files, use their own E-mail encryption solution, or contact their district examiner on how to use NCUA's encryption solution.

Additionally, on occasion un-solicited sensitive information may come into OCCU staff's possession (e.g., an entity sends something to NCUA unsolicited, either electronically or hardcopy). These items are properly secured upon receipt and destroyed when no longer needed for agency purposes.

In summary, to prevent disclosure to unauthorized parties, OCCU examiners follow specific procedures to safeguard your corporate credit union's confidential and sensitive information.

If you have any questions or concerns, please contact OCCU at 703-518-6640.

Sincerely,

Scott Hunt
Director
Office Corporate Credit Unions

cc: State Supervisory Authorities
NASCUS
NAFCU
ACCU