NCUA LETTER TO CREDIT UNIONS

NATIONAL CREDIT UNION ADMINISTRATION
1775 Duke Street, Alexandria, VA 22314

DATE: **February 2003** **LETTER NO.:** **03-CU-03**

TO: **All Federally-Insured Credit Unions**

SUBJ: **Wireless Technology**

The purpose of this letter is to provide important considerations for credit unions that are currently engaged in or may be considering the use of wireless technology.

Wireless technology can potentially provide important benefits for credit unions and their members. For some, this may be a cost-effective alternative for a credit union seeking to expand its existing hard-wired computer network. Additionally, it may enable a credit union to provide members with increased accessibility to its Internet-based financial service offerings.

However, those credit unions that have made a decision to implement wireless technology should also be aware of the potential increase in the amount of risk exposure for the credit union. Credit unions may be able to mitigate the following risk areas with proper planning and controls:

- **Strategic Risk** – A credit union's ability to meet its strategic goals for wireless technology may be impacted due to:
  - adverse business decisions (e.g., accurate identification of likely demand is critical prior to the technology investment);
  - poor implementation (e.g., research of technical and security issues should be completed prior to implementation); or
  - lack of responsiveness to changes in the environment (e.g., likelihood and timing of future system upgrades necessitated by rapidly changing standards should be carefully evaluated).

- **Transactional Risk** – A credit union's ability to securely deliver wireless services and manage information may be impacted due to:

- fraud (e.g., adequate protections should be in place to protect against fraudulent transactions, as well as theft, destruction, and manipulation of member or credit union data);
- error (e.g., scope of testing should be commensurate with the risk inherent in the service and should be conducted prior to full implementation); or
- system reliability (e.g., testing should be completed to determine if the likelihood of disruption of services due to interference from other wireless devices on similar radio frequencies is within tolerable limits established by credit union).

- **Compliance Risk** – A credit union could face the potential of fines, civil money penalties, payment of damages, contract voidance, and diminished reputation due to violations of, or nonconformance with:
  - laws, rules, or regulations (e.g., development of a written security program is required by Part 748 of the NCUA Rules and Regulations *Security Program, Report of Crime and Catastrophic Act and Bank Secrecy Act Compliance*);
  - prescribed practices (e.g., development and implementation guidelines for a member information security program are outlined in NCUA Part 748 of the NCUA Rules and Regulations Appendix A *Guidelines for Safeguarding Member Information*); or
  - policies and procedures (e.g., internal security protocols should be monitored and enforced to enhance effectiveness).

- **Reputation Risk** – A credit union could potentially encounter negative public opinion due to inadequate management of the strategic, operational, and compliance risks outlined above. Adequate management of these risks should reduce the threat of a loss in member confidence in the credit union and/or its wireless services.

NCUA encourages credit unions to review the guidance below to assist with the planning, contracting, implementing, and monitoring of wireless technology.

1. **NCUA Letter to Credit Unions 01-CU-11 *Electronic Data Security Overview*.** This document outlines regulatory requirements and the development and implementation of a security program for electronic data and information systems. The Letter can be obtained via the Information Systems and Technology (IS&T) link found on the Reference page of NCUA's website, www.ncua.gov.

2. **Attachment to the Federal Deposit Insurance Corporation's Financial Institution Letter FIL-8-2002 *Wireless Networks and Customer Access*.** This document identifies specific threats associated with wireless technology and related mitigation methods. This information is applicable to credit unions as well as banks. It can be obtained via the Financial Institution Letters link on the FDIC's website, www.fdic.gov.

3. **The National Infrastructure Protection Center's (NIPC) "Best Practices for Wireless Fidelity (802.11b) Network Vulnerabilities" publication.** This publication is technical in nature and is best suited for those individuals responsible for the technical planning, implementation, and evaluation of wireless. It outlines wireless security issues and related recommendations from the wireless industry. It can be obtained via the "Other Publications" link under the "Publications" link on NIPC's website, www.nipc.gov.

   This NIPC document contains an inactive link to the Wireless Ethernet Compatibility Alliance's (WECA) Wired Equivalent Privacy (WEP) Security Statement. WECA is now known as the Wi-Fi Alliance. Its recommended security practices can be obtained via the "Design Your Network" and "Secure Wi-Fi" tabs under the "About Wi-Fi" tab on the Wi-Fi Alliance's website, www.wi-fi.com. Depending on your web browser's configuration, you may need to navigate the site using the "Site Map" link on the bottom of the main page.

If you have any questions, please contact your NCUA Regional Office or State Supervisory Authority.

Sincerely,

/S/

Dennis Dollar
Chairman