Farm Credit Administration

1501 Farm Credit Drive
McLean, Virginia 22102-5090
(703) 883-4000

INFORMATIONAL MEMORANDUM

December 17, 2002

To: The Chief Executive Officer
All Farm Credit System Institutions

From: Roland E. Smith, Director
Office of Examination

Subject: Alert: Managing Risks Associated with Wireless Networks and Customer Access

Wireless technologies offer Farm Credit System (FCS) institutions an alternative means to reach customers and reduce the costs of implementing new networks. But, FCS institutions considering implementation of this still relatively new technologies should be mindful of the risks associated with wireless technologies and take appropriate steps to manage those risks.

Implementation of Wireless Technologies

Wireless networks have become a cost-effective alternative for providing network connectivity to financial institution information systems. The installation costs of wireless networks compares quite favorably to traditional network wiring and may be especially attractive in rural areas. Recent performance enhancements in wireless technologies have increased operating speeds, allowing wireless networks to easily integrate with an institution's existing wired networks.

An increasing number of consumers are using wireless technologies to access banking applications. Wireless Internet access is a fairly common feature on new cellular phones and hand-held computers, thereby further increasing the potential number of customers using those applications.

Wireless technologies present FCS institutions some of the same risks that exist with traditional wired networks. But wireless technologies also contain additional risks which institutions must factor into the design, implementation, and operation of a wireless network. Those risks include:

- Compromise of customer information and transactions over the wireless network;
- Intrusion into the institution's networks though wireless network connections;
- Disclosure of confidential customer information to unauthorized parties (identity theft); and
- Obsolescence of current systems because of rapidly changing wireless industry standards.

These risks could ultimately compromise the institution's computer system and potentially cause financial loss due to the execution of unauthorized transactions. In addition, the risks associated with wireless technologies could severely harm the institution's reputation and cause a loss of customer confidence.

Risk Mitigation of Wireless Technologies

Compared to traditional wired networks, current wireless networks provide for a less secure environment. FCS institutions considering implementing wireless technologies should carefully evaluate the associated risks and determine the steps necessary to lessen those risks. Those steps should include:

- Determining the cost and benefit of incorporating wireless technologies into their business operation;
- Adopting procedures that address and adequately mitigate the specific security weaknesses found in the wireless environment;
- Establishing a minimum set of security requirements for wireless networks and applications;
- Adopting encryption processes that ensure end-to-end encryption of information that passes through the wireless network; and
- Performing independent security testing of wireless network and application processes.

As wireless technologies evolve, the security and control features available for financial institutions will make the process of risk mitigation easier. In the meantime, utilization of wireless technologies should be approached with caution and care.

If you have any questions about this memorandum, please call Tom Glenn, Special Examination and Supervision Division, Office of Examination, at (703) 883-4412, or write to him on the Internet at e-mail address *Glennt@fca.gov.*