Farm Credit Administration

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

INFORMATIONAL MEMORANDUM

October 2, 2000

To: The Chief Executive Officer
All Farm Credit System Institutions

From: Cheryl Tates Macias
Chief Operating Officer

Subject: E-commerce and Security Risks

Farm Credit System (FCS) institutions are increasingly becoming engaged in electronic commerce (E-commerce). FCA examiners recently completed two Web site reviews that show the number and sophistication of FCS Web sites have increased substantially in the last year. Recent legislation, "Electronic Signatures in Global and National Commerce Act" (E-SIGN) (Public Law 106-229), makes it easier for FCS institutions to engage in E-commerce. FCA Bookletter (BL-041) on E-SIGN addresses the legal validity (with some exceptions) of electronic contracts, electronic signatures, and records maintained in electronic rather than paper form. At the same time, the Internet presents significant security risks.

FCS institutions should ask the following questions about security risks of E-commerce and ensure that policies and practices are in place to control these risks. You may expect our examiners to ask these or similar questions about your E-commerce activities in the near future.

Does your institution keep data private? Unless protected, everything sent over the Internet is open and anyone can read it. Also, storage systems connected to the Internet may be vulnerable if not properly secured.

How do you keep data in its original or intended form? People with the appropriate skills and tools can change data during transmission. Also, a user could compromise data integrity within a data storage system, intentionally or unintentionally.

Do you verify the identity of the parties in a transaction? It is easy for someone to impersonate or misrepresent their identity. For example, someone can send E-mail and make it look like someone else sent it.

Can your institution prevent parties in an online transaction from falsely denying they created, sent, or received communications? Institutions must protect themselves against a false denial that someone did not receive the data or a false denial that someone did not send the data.

Does your institution have strong security measures to control access? Because a computer network's security is only as strong as its weakest link, management must protect all systems from attack and unauthorized access. Your institution should be able to answer "yes" to the following questions related to access control issues:

- Does your institution have adequate procedures to prevent it from being used or being a target in denial of service attacks? A denial of service attack can bring down a network server by overwhelming it with so many requests that it shuts down.

- Has management set up permissible activities? Management should disable all impermissible activities. For example, the File Transfer Protocol (commonly referred to as FTP) that allows the transfer, copying, and deleting of files between computers may be unnecessary. Another protocol, Telnet, enables one computer to log in to another and can be dangerous. Technologies such as Java and Active X present security concerns, and institutions should limit their use.

- Does management use experts and software programs to perform security scans to identify weaknesses? Security tools for the network administrator are freely available on the Internet, and intruders may use them to exploit network vulnerabilities.

- Has management adopted a strong password policy? Sophisticated intrusion tools can find and decipher passwords. Common passwords set by the product manufacturer (default passwords) are widely known for specific products. A password policy should incorporate expiration and lockout rules. It should also require disabling default accounts.

- Does the institution have procedures to track and install important software patches? Often, people identify security problems in software products. Manufacturers release patches to correct flaws.

- Is virus protection software kept current? People constantly introduce new computer viruses that may damage data or disable systems. The most effective protection is routinely updating protection software, combined with educating users.

Does your institution have a mechanism to detect a breach of security and report it to appropriate law enforcement agencies and the FCA? Do you have policies to guide the institution in its response to system intrusions? FCS institutions are required to report known or suspected criminal violations, including computer intrusions, under 12 C.F.R. Part 617.

Technologies and services such as encryption, digital signatures, and firewalls can mitigate many of the risks identified in the questions above. These technologies are not a substitute for knowledgeable and actively involved management and users. As a good business practice, institutions should educate users about the risks to systems. Management also should educate itself to ensure the business risks associated with systems are equal to the benefits of the system. As technologies change and security controls improve, so will the tools and methods used by others to compromise data and systems. Management must not only impose comprehensive security controls but also constantly guard against current and emerging threats.

If you have any questions regarding this Informational Memorandum, please contact Thomas Glenn, Special Examination and Supervision Division, Office of Examination, at (703) 883-4412, or correspond on the Internet at E-mail address glennt@fca.gov.