RB-1999-01 Guidance on Electronic Financial Services

BACKGROUND

Increasingly, credit unions are exploring business opportunities presented by technology, the Internet, and the World Wide Web. Credit unions are exploring these electronic areas to remain competitive, improve member service, and reduce their operating costs. As a general rule, credit unions do not have to inform the Department before using such electronic means and facilities for activities that they are otherwise authorized to perform or provide. Credit unions are, however, required to file a written notice with the Department before establishing a transactional web site and follow any procedures imposed in writing by the Department in response to any supervisory or compliance concerns that may affect your use of electronic means or facilities.

While electronic services will provide important benefits to credit unions and their members, they also will expose credit unions to new and different risks. As credit unions increase their dependency on technology to deliver services and process information, the risk of adverse consequences from operational failures increases. A credit union's effectiveness in controlling the risks inherent in the use of evolving technologies is directly related to its overall safe and sound operations. Credit unions that offer electronic financial services should create a safe, sound, and secure infrastructure that is adequate to mitigate risks associated with such activities. The Department will review technology-related risks together with all other risks to ensure that a credit union's risk management is integrated and comprehensive.

RISK AND CONTROLS

Before implementing an electronic financial services program, management should exercise due diligence and develop comprehensive plans to identify, assess, and mitigate potential risks and establish prudent controls. Such due diligence and planning would typically include the following activities:

- Review the implications of electronic financial services on the credit union’s business plan;
- Evaluate member expectations and demands;
- Evaluate internal and external expertise and resource requirements to support the electronic financial services;
- Assess the risks and required controls, particularly those related to system security; and
- Develop effective policies and procedures that cover the program.

Electronic financial service activities involve a wide range of potential risks. Some of these are unique to the delivery channel, while others represent general concerns that are common to traditional credit union practices. When implementing electronic financial services, as with any new program, management must ensure that unique areas are identified and addressed. For example, new computer hardware and software may be needed to control security threats, while existing audit procedures will require expansion to incorporate the new system.

In general, electronic services related risks can be categorized as Strategic, Reputation, Compliance, and Transactional. Within these general risk areas, there are several concerns that are unique to electronic financial services. These categories are not mutually exclusive and each of the general risk areas are discussed more fully below, along with some examples of compensating controls

Strategic Risk

Strategic risk exists in the business decisions that a credit union faces when new products or services are introduced. Specifically, this is the risk to earnings or capital arising from adverse business decisions or improper implementation of those decisions. The issues that each credit union should address for any new product or service are: (1) the development of a business plan which justifies the program; (2) availability of sufficient resources to support the program; (3) whether to outsource certain functions or perform them in-house; and (4) staying abreast of technological developments.

Business Plan

The decision to offer an electronic financial service program should be justified by a positive business plan. In developing the business plan, management should:

- Conduct Research and Consult with Experts – Management should consult with qualified technology, legal, economic, audit, regulatory, and other experts to evaluate pertinent issues.
- Perform Strategic Technology Planning – Technology planning is part of the strategic planning process. Credit unions should clearly define its goals and objectives in this area and allocate sufficient resources.
- Establish Goals and Monitor Performance – Performance goals measure the success of the electronic financial services program. The program should be reevaluated periodically in light of strategic plan modifications, member satisfaction and new technologies.

Internal and External Resources

The availability and cost of additional resources (internal and external) should be evaluated to determine their sufficiency relative to the demands of the electronic financial service program. The resources should be sufficient to:

- Provide Adequate Training – The credit union's staff should be properly trained to implement the program. Specifically, they should be educated on new security procedures and control practices. Qualifications of external personnel should be evaluated prior to contracting with the vendor.
- Provide Adequate Support Staff – Support staff (e.g., call center staff and customer service representatives) should be kept informed of any changes or updates to the program. Additional personnel may be needed to address an increased volume of member inquiries.
- Maintain Software Updates – Software changes require administrative controls. Credit unions may have to rely on members to install end-user software updates and accommodate those who are unable or unwilling to upgrade. Multiple software versions may have to be supported.
- Establish Adequate Insurance Coverage – Insurance providers should be consulted to confirm adequate coverage for electronic financial services activities.
- Monitor Inter-relationships – Inter-relationships among multiple financial institutions, vendors or originators, and participants within a payment system should be monitored to ensure transactions are completed in their entirety.

Outsourcing Arrangements

Outsourcing arrangements are commonly used for many aspects of

electronic financial services programs. However, such arrangements must be properly initiated, documented, and managed. Insufficient control over a vendor can result in potential liability and embarrassment to a credit union. When a credit union plans to outsource part or all of its electronic financial services, it should:

- Perform Due Diligence on Vendors – Select only vendors who are knowledgeable of the emerging technology. Management should consider the vendor's financial condition and ability to provide ongoing services. It would also seem prudent to have the credit union's attorney review all contracts.
- Monitor Performance – The performance of the vendor should be monitored and compared to the provisions of the contract.
- Establish Back-up Arrangements – The possible inability of a vendor to fulfill its obligation should be considered by management. The degree of difficulty and cost to obtain a replacement should determine the extent to which back-up arrangements are considered.

Technological Developments

The dynamic nature of technology makes it incumbent on credit unions to maintain secure systems that meet member needs. A credit union's information technology plan should include consideration of future system upgrades as more sophisticated security techniques and user options are developed. To help ensure a secure electronic financial services program that continues to meet member needs, management should:

- Monitor New Developments – Schedule periodic evaluations of new technologies in hardware and software. Management should evaluate new products, services, and vendors against business plans and in light of the aforementioned risks.
- Budget for Technology Upgrades – Consideration should be

given to the costs of technological upgrades to maintain appropriate security and adapt to member expectations.

Compliance Risk

Compliance risks arise from the uncertainty of how the electronic environment will affect legal framework, jurisdiction, and regulatory compliance. Specifically, this is the risk to earnings or capital arising from violations of, or non-conformance with, laws, rules, regulations, prescribed practices, or ethical standards. Compliance risks expose the credit union to fines, civil money penalties, payment of damages, and the voiding of contracts. Compliance countermeasures generally consist of effective policies and procedures and comprehensive disclosures.

As credit unions move increasingly from paper to electronic-based transactions and information exchanges, they need to consider how laws designed for paper-based transactions apply to electronic-based transactions and information exchanges. Some new technologies raise unexpected compliance issues. Transactions conducted through the Internet also can raise novel questions regarding jurisdictional authority over those transactions. Therefore, credit unions should be careful to monitor and respond to changes to relevant laws and regulations arising from these developments.

Regulatory Compliance

The existing regulatory framework remains applicable in the electronic environment, but may require new interpretations. Management should consider the ramifications of members residing in distant locations who may have no physical contact with the credit union. At a minimum, management should:

- Update Policies and Procedures – Policies and procedures should be modified as needed to incorporate the electronic financial services program.

- Expand Internal and External Audit – Programs to monitor compliance with regulatory requirements should be expanded to include electronic delivery channels. Audit trails should be incorporated into each program or system. Ensure advertisements for products and services contain the proper disclosures in accordance with any federal or state laws.

Legal Framework

Many basic legal questions complicate electronic financial activities. The applicability of existing laws in an electronic environment is uncertain in many cases and credit unions must exercise caution when addressing legal issues related to electronic financial services. Management should consider:

- Detailed Contracts – When certain functions of electronic financial services are outsourced, detailed contracts are used to define the roles and responsibilities of the credit union and vendors. Contracts should include delineations of authority, responsibilities, and accountability; provide protective covenants; and address confidentiality, ownership of credit union records, and safety of members assets.
- Disclosures – Management should ensure that members are fully informed of the risks associated with their participation in an electronic financial services program. Member disclosures should explain the circumstances under which their account data may be at risk and the security methods employed by the credit union. Members must be informed of their rights and responsibilities in the event of unauthorized access.
- Privacy Issues – The Internet opens the door to new opportunities for credit unions; however, to capitalize on those opportunities, credit unions must reassure members that the credit union-member relationship – and

the expectation of privacy that is an essential part of that relationship – will be honored as much on the Internet as it is in the branch office.

Transactional Risk

Transactional risk arises from the potential that inadequate information systems, operational problems, breaches in internal controls, fraud, or unforeseen events will result in unexpected losses. The integrity of data that is transmitted, processed, and stored must be protected from unauthorized access. Electronic financial services involve the use of delivery channels (e.g., public telephone networks and the Internet) that are generally outside the credit union's control. The global reach of these systems and the number of uncontrolled access points introduces heightened transactional risk. However, programs can be implemented to prevent, detect, and contain a system attack and protect confidential data.

Security

Security is the paramount issue, since access represents an opening of the computer system to outside and potentially unauthorized users. Although the devices and distribution channels may vary, the risk and control issues delineated in this document are generally applicable regardless of the type of access device or distribution channel.

System security requires implementation of proper controls to guard against unauthorized access to the credit union's networks, systems, and databases. Management should control user access to prevent a security compromise of internal systems. Member data must be protected from unauthorized access or altercation during transmission over public networks. Management should develop methods to maintain confidentially, ensure the intended person receives accurate information, and prevent eavesdropping by others. In addition, to ensure non-repudiation, undeniable proof of participation

by both the sender and the receiver in a transaction must be created. Controls that management could implement include:

- Authorization – Authorization involves the pre-determination of permissible activities. Management should ensure that members have access only to their own accounts and perform only authorized functions.
- Access Control – Traditional access controls, such as user identification, passwords, and personal identification numbers, should be implemented for members using electronic financial services. However, since the effectiveness of these controls is greatly influenced by the member, management should take all possible steps to educate the members in this area.
- Authentication – Authentication is used to verify and recognize the identity of parties to a transaction. Credit unions may communicate with members they never physically meet resulting in opportunities for misrepresentations. Authentication is the primary component of non-repudiation.
- Secure Data Storage – Confidential information or highly sensitive data should be stored securely. Management should consider storing sensitive data in encrypted form and implementing stringent access controls.
- Encryption – Encryption technology disguises information to hide its meaning and enhances confidentiality by restricting information access to only intended users. Encryption-based methods can also be used to verify message authenticity and accuracy. Information is encrypted and decrypted with a cipher and key using specialized computer hardware or software. Secrecy of the key and complexity of the cipher are crucial for the success of encryption controls.
- Firewalls – Firewalls are physical devices, software programs, or both, that enhance security by monitoring and limiting access to computer facilities. They create a security barrier between two or more networks to

protect the credit union's computer system from unauthorized entry. Filtering routers may be incorporated into the firewall system to screen data traffic and direct messages to certain locations.

Reputation Risk

Reputation risk is the risk to earnings or capital arising from negative member opinion. This affects the credit union's ability to establish new relationships or services, or to continue servicing existing members.

Reputation risk arises whenever electronic products, services, delivery channels, or processes may generate adverse public opinion such that it seriously affects a credit union's earnings or impairs capital. Examples may include: flawed security systems that significantly compromise member privacy; inadequate contingency and business resumption plans that affect a credit union's ability to maintain or resume operations and to provide member services following system failures; fraud that fundamentally undermines member trust; and large-scale litigation that exposes a credit union to significant liability and results in severe damage to a credit union's reputation. Adverse member opinion may create a lasting, negative image of overall credit union operations and thus impair a credit union's ability to establish and maintain member and business relationships.

Operations

System reliability requires that all aspects of the system are available and function as promised. Management should consider the risks created by reliance on systems whose performance is beyond their control. For example, management has little or no control over the performance of the Internet. System capacity and resource adequacy are considerations in meeting existing and anticipated volume. Consistency of operations should be ensured, including plans for recovery from service

disruptions. To ensure the credit union has a reliable electronic financial services program, management should establish:

- Policies and Procedures – Policies can be used to delineate the board's expectations, benchmarks, and standard operating procedures.
- Contingency Plans – Contingency plans can be used to minimize business disruptions caused by problems that impair or destroy the credit union's processing and delivery systems. The plan should be tested periodically.
- Audit Procedures – The system should be auditable and designed with attention to controls, including segregation of duties. Qualified internal and external auditors should evaluate the system's controls periodically.

CONCLUSIONS

This guidance provides information for credit unions to consider during the design, development, implementation and monitoring of an electronic financial services program. The Department expects credit unions to identify, measure, monitor, and control its electronic-related risks and, as with all other risks, to avoid excessive exposure that may threaten the safety and soundness of the institution. Because electronic-related risks are important factors in assessing a credit union's overall risk profile, the Department's primary supervisory concern in reviewing a credit union's use of electronic services is whether the credit union is assuming a level of risk that exceeds its ability to manage and control the risk.

The Department understands and appreciates that credit unions currently address their electronic-related needs in different

ways. For example, some credit unions incorporate technology planning into their overall strategic plans while others deal with technology applications on a project-by-project basis. The sophistication of the risk management process should be appropriate for the credit union’s level of risk exposure. This includes the materiality of the risks, the degree of risk posed by electronic services as compared to, and when aggregated with, other credit union risks, and the overall ability of the credit union to manage and control its risks. Regardless of the specific credit union approach, sound risk management systems have several common fundamentals: risk identification, risk measurement, risk control, and risk monitoring.

[1] The provisions of Commission Rule 91.5005 were adopted to be effective March 13, 2006 and replaced Commission Rule 91.401(b).