Section 2226
Home Banking
Northern Lights Federal Credit Union
Home Banking/Internet Banking Policy

Purpose:

The purpose of this policy is to establish guidance on how to identify, measure, monitor, and control risks arising from the use of PC banking, i.e., Internet Banking, which incorporates the use of personal computers. It also sets forth the expectations of company management and NLFCU's Board of Directors when implementing and operating Internet Banking systems.

Introduction

Internet banking presents opportunities and challenges for NLFCU. It provides a delivery channel that allows the credit union to provide services to an expanded geographic region while increasing customer convenience and reducing transaction costs. Internet banking allows customer access to NLFCU's internal systems via public networks, such as the Internet , and, although there are security issues, these security issues will be considered and managed in a prudent manner. The management and Board of Directors of NLFCU have made a significant commitment to the financial institution's Internet banking system and expect this system to be a key factor in attracting and retaining customers.

Internet banking necessitates a reliance on service providers and software vendors to design, implement, and manage Internet banking systems. NLFCU has elected to operate its Internet banking system through Northern Data Systems (SHARETEC) as part of its core system. The credit union recognized that, as with any outsourced product of service, reliance on service providers and software vendors for Internet banking requires sound risk management practices and vendor due diligence.

Internet banking risks and controls

Internet banking systems primarily expose financial institutions to transaction, strategic, reputation, and compliance risk, but may expose NLFCU to other risks as well. For example, Internet banking systems represent credit risk as NLFCU offers lending or new account services over the Internet. NLFCU currently offers applications for new accounts and lending services inside of our Internet banking product. Applications are carefully reviewed and identification of applicants must be verified either through personal contact and identification of known customers or through the use of notarized signatures on any final documents. "Know your customer" considerations in this context requires the use of different identification, authentication, and transaction verification methods than those used with traditional delivery channels. NLFCU limits applications for new accounts and lending services to its local market area, and posts this information on all related Internet banking screens and applications. Documents requiring signatures, such as final notes for loans or signature cards for new accounts, require the client to meet with a financial institution representative and/or be verified as outlined in the financial institution's new account procedures or, in special circumstances, to have the document notarized and submitted to the credit union. Liquidity, interest rate, market, price, and foreign exchange risks may result from poor data integrity or unreliable systems. NLFCU posts current rates on its web site for the convenience of its customers and prospects, but limits applications to its designated market area. NLFCU does not offer foreign exchange through its Internet banking service.

Internet banking risks are managed as part of the credit union's overall risk management process. NLFCU uses a rigorous analytic process to identify, measure, monitor, and control risks. The quantity of risk assume should be consistent with the credit union's overall risk tolerance and must not exceed the credit union's ability to manage and control its risks. Management and staff are expected to have the knowledge and skills necessary to understand and effectively manage Internet banking-related risks.

NLFCU uses Northern Data Systems (Sharetec) as our software vendor and processor to provide Internet banking services. Management and the board of directors performed extensive due diligence on this vendor before selecting it as our Internet banking system provider. We believe that NDS has a very good reputation, financial status, and viability. Having a strong relationship with our vendor helps ensure that it performs as promised and that it not only capable of keeping abreast of new or changing technology, but also committed to doing so. We have controls in place to monitor performance levels and to swiftly respond to any problem or emergency. This monitoring is ongoing and will continue to improve over time as our Internet banking service mature. Control items should include, but not be limited to, our credit union's ability to perform audits, either internally and/or on an outsourced basis, or to obtain from the service provider or software vendor copies of their independent internal control audits.

The Internet banking product server is maintained at NLFCU's data center. Files are extracted from our core system and pushed from this server. NLFCU has a firewall that sits between the Internet and its local LAN. Its LAN is connected to an EVC line that provides access to our server. The firewall denies any direct access from the Internet through the use of security policies that do not allow public Internet traffic to reach the LAN. NLFCU receives data from the Internet due to a policy in the firewall that allows traffic that is initiated from the

LAN to the Internet to pass but not vice versa.

As NLFCU's Internet banking provider, NDS has primary responsibility for physical security, maintenance, and current levels of software.

Transaction risk

Transaction risk is the most common source of risk arising from Internet banking. It results from weaknesses in design, implementation, and monitoring. NLFCU will ensure that personnel are properly trained on new technology to the extent required. Recognizing that NLFCU does not have on staff the necessary expertise or resources to design and implement a secure and reliable system, management has carefully selected and appropriate vendor – Northern Data Systems (NDS) - and elected to assist in managing its systems. .

Information security is critical to the safe and sound operation of Internet banking systems. Connections and public networks, such as the Internet, can expose the institution to significant security challenges, including unauthorized users and intrusions, system failures, access and data privacy issues, and computer viruses.

Control and security

NLFCU's security program should provide "end-to-end" security controls for critical data and critical facilities. (Note: end-to-end security provides company-wide implementation of physical and data controls to protect the credit union's critical information, human resources, and physical assets from internal or external intrusion or compromise.)

Management of NLFCU should ensure that periodic security risk assessments are conducted to identify internal and external threats that may undermine data integrity, interfere with service, or result in the destruction of information. Threat and vulnerability assessment findings assist management with decisions regarding the types and configuration of security controls. Threats may come from criminal enterprises, hackers, or disgruntled or unethical employees. Careless or improperly trained staff or users of Internet banking systems also can pose security risks. Computer viruses may corrupt data or cause systems to fail. Controls should be implemented to maintain data integrity and to promote privacy and confidentiality. to assess the credit union's security program, management will ensure that an objective and qualified independent source reviews and tests the controls to ensure their effectiveness.

Security controls

Management has developed security controls that govern network and data access user authentication, transaction verification and virus protection.

Network and data access controls

Access control allow verification and enforcement of a user's authorized right to access the credit union's network, applications, and data. Thorough user authentication will identify internal and external users of our networks.

User authentication (members)

Authentication is the process of determining whether Internet banking system users are who they claim to be. In general, the credit union will identify the customer before issuing authorization codes. Once the customer has been identified, the credit union will assign a password. The customer will need to change the password immediately the first time they attempt to use their password. Members are not allowed to use common information on which to base their password such as social security, address, phone number, etc.

Password

Passwords are assigned to control access to Internet banking systems and should help to ensure the integrity of passwords by providing instruction on their proper use and protection. Specifically, we consider the following password protection practices:

1 Minimum five character length for passwords.
2 Use of alpha, numerical, alphanumeric, or special characters passwords is required.
3 Users must call the Customer Service Department to have user passwords and identifications reset.
4 Session controls automatically logoff after three failed access attempts.
5 User ID and passwords are encrypted during transmission.

Firewalls combine software to block unwanted communications into and out of the credit union's network, while allowing acceptable communications to pass. The router and firewall software is pre-configured by the credit union's Internet banking provider to allow access to information only through a designated network card. This provides protection of the credit union's internal network and protects all connection points between the internal network and external networks, such as the Internet. The firewall position is based on the desired level of security as dictated by the credit union's risk assessment and data classification efforts. Firewall design and implementation is complex, so NLFCU allows both its Internal banking system provider and its Information Systems auditor to certify the configuration. The credit union's Internet banking system vendor maintains the effectiveness of its firewalls from an objective qualified internal and external source with adequate security expertise. NLFCU's Information Systems auditor will conduct periodic review and testing of firewalls.

Encryption transforms data into an unreadable format. The credit union's system uses 128-bit encryption for all Internet banking system communications. Encryption is used when transmitting all sensitive or critical data. The strength of encryption depends on a combination of three elements: a mathematical algorithm, key length, and the confidentiality of the key used to encode the message.

Transaction verification

NLFCU's Internet banking provides audit trails that are maintained for purposed of identifying the parties that initiate transactions. Audit trails enable the credit union or its Internet banking vendor to verify specific transactions and can provide proof of transactions to avoid claims of repudiation by customers.

Virus protection

NLFCU has established a company-wide detection and prevention program to reduce the likelihood of computer viruses. This includes end-user polices, training and awareness programs, virus detection tools, and enforcement procedures.

Security monitoring

NLFCU places a strong emphasis on using monitoring tools to identify vulnerabilities and, in a real-time mode, detect possible intrusions from external and internal parties (e.g. hackers). As provided in the credit union's security policy, staff should report security breaches promptly to appropriate management and external officials. We have contracted with an outside firm that specializes in monitoring security for credit unions to conduct penetration testing and administer manual or automated intrusion detection processes.

Penetration testing

Penetration testing is the process of identifying, isolating, and confirming possible flaws in the design and implementation of passwords, firewalls, encryption, and other security controls. Tests simulate the probable actions of unauthorized and authorized users. Because the tactics used by unauthorized users to infiltrate computer systems frequently change, penetration tests to not guarantee that firewalls will prevent all types of attacks. By using a third party, NLFCU has ensured that testing is conducted by an objective and qualified independent source at least annually or whenever substantial changes are made to the Internet banking security systems. The credit union's Internet banking vendor also has penetration testing conducted by a third party and provides results of these tests to management of NLFCU. NLFCU has obtained complete information regarding disaster recovery tests, penetration tests, external audits, and etc. to ensure the NLFCU management, auditors, and regulators can appropriately evaluate the security of these systems and the vendor's commitment to ensuring security and compliance. Additionally, NLFCU has contracted with a firm specializing in financial institution network design, consulting, and testing to provide annual network reviews and consulting.

Intrusion detection

Transaction and audit logs can be produced through firewall technology and can be used to detect network activity or intrusions. There are automated intrusion detection devices available that monitor network traffic on a real-time basis. NLFCU has contracted with NDS to provide an intrusion detection system where transactions activity can be effectively monitored through manual processes or systems.

Following the detection of an unauthorized act or user, the financial institution will initiate procedures to respond to the intrusion. If a security breach occurs that may result in serious reputation damage or financial loss, security administrators should alert senior management, and

the Board of Directors concerning the cause and scope of the breach. They also will discuss the extent of damage or disclosure of information, and what risks, including legal liability, the credit union may incur. Response activities should include communications and customers, and where appropriate, law enforcement agencies, regulatory agencies, and the media.