RB-2000-02 Guidance on Information System Security

BACKGROUND

The purpose of this Bulletin is to provide credit unions with background information and guidance on various risk assessment tools and practices related to information security. Credit unions using the Internet or other computer networks are exposed to various categories of risk that could result in the possibility of financial loss and reputational harm. Given the rapid growth of the Internet and networking technology, the available risk assessment tools and practices are becoming more important for information security.

This Bulletin provides a summary of critical points, discusses components of a sound information security program, and describes the risk assessment and risk management processes for information security. The appendix provides specific information on certain risk assessment tools and practices that may be part of a credit union's information security program. The Bulletin and appendix are intended to provide useful information and guidance, and not to create new examination standards, impose new regulatory requirements, or represent an exclusive description of the various ways credit unions can implement effective information security programs.

Whether credit unions contract with third-party providers for computer services or maintain computer services in-house, credit union management is responsible for ensuring that systems and data are protected against risks associated with emerging technologies and computer networks. If a credit union is relying on a third-party provider, management must generally understand the provider's information security program to effectively evaluate the security system's ability

to protect credit union and member data.

The Department has previously issued guidance on information security concerns. This Bulletin is designed to supplement Regulatory Bulletin 1999-01, “Guidance on Electronic Financial Services,” dated September 1, 1999, and to complement the Department’s soon-to-be implemented electronic commerce examination procedures.

SUMMARY OF CRITICAL POINTS

To ensure the security of information systems and data, credit unions should have a sound information security program that identifies, measures, monitors, and manages potential risk exposure. Fundamental to an effective information security program is an ongoing risk assessment of threats and vulnerabilities surrounding networked and/or Internet systems. Credit unions should consider the various measures available to support and enhance information security programs. The appendix to this Bulletin describes certain vulnerability assessment tools and intrusion detection methods that can be useful in preventing and identifying attempted external break-ins or internal misuse of information systems. Credit unions should also consider plans for responding to an information security incident.

INFORMATION SECURITY PROGRAM

A credit union’s board of directors and senior management should be aware of information security issues and be involved in developing an appropriate information security program. A comprehensive information security policy should outline a proactive and ongoing program incorporating three components:

- Prevention
- Detection
- Response

Prevention measures include sound security policies, well-designed system architecture, properly configured firewalls, and strong authentication programs. This Bulletin discusses two additional prevention measures: vulnerability assessment tools and penetration analyses. Vulnerability assessment tools generally involve running scans on a system to proactively detect known vulnerabilities such as security flaws and bugs in software and hardware. These tools can also detect holes allowing unauthorized access to a network or insiders to misuse the system. Penetration analysis involves an independent party (internal or external) testing a credit union's information system security to identify (and possibly exploit) vulnerabilities in the system and surrounding processes. Using vulnerability assessment tools and performing regular penetration analyses will assist a credit union in determining what security weaknesses exist in its information systems.

Detection measures involve analyzing available information to determine if an information system has been compromised, misused, or accessed by unauthorized individuals. Detection measures may be enhanced by the use of intrusion detection systems (IDSs) that act as a burglar alarm, alerting the credit union or service provider to potential external break-ins or internal misuse of the system(s) being monitored.

Another key area involves preparing a *response* program to handle suspected intrusions and system misuse once they are detected. Credit unions should have an effective incident response program outlined in a security policy that prioritizes incidents, discusses appropriate responses to incidents, and establishes reporting requirements.

The appendix provides a detailed discussion on prevention (vulnerability assessment tools and penetration analyses), detection (IDSs tools), and response measures. Before implementing some or all of these measures, a credit union should perform an information security risk assessment.

Depending on the risk assessment, certain risk assessment tools and practices discussed in this Bulletin may be appropriate. However, use of these measures should not result in decreased emphasis on information security or the need for human expertise.

RISK ASSESSMENT/MANAGEMENT

A thorough and proactive risk assessment is the first step in establishing a sound security program. This is the ongoing process of evaluating threats and vulnerabilities, and establishing an appropriate risk management program to mitigate potential monetary losses and harm to a credit union's reputation. Threats have the potential to harm a credit union, while vulnerabilities are weaknesses that can be exploited.

The extent of the information security program should be commensurate with the degree of risk associated with the credit union's systems, networks, and information assets. For example, compared to an information-only Web site, credit unions offering transactional electronic activities are exposed to greater risks. Further, real-time funds transfers generally pose greater risks than delayed or batch-processed transactions because the items are processed immediately. The extent to which a credit union contracts with third-party vendors will also affect the nature of the risk assessment program.

Performing the Risk Assessment and Determining Vulnerabilities

Performing a sound risk assessment is critical to establishing an effective information security program. The risk assessment provides a framework for establishing policy guidelines and identifying the risk assessment tools and practices that may be appropriate for a credit union. Credit

unions should have a written information security policy, sound security policy guidelines, and well-designed system architecture, as well as provide for physical security, employee education, and testing as part of an effective program.

When credit unions contract with third-party providers for information system services, they should have a sound oversight program. At a minimum, the security-related clauses of a written contract should define the responsibilities of both parties with respect to data confidentiality, system security, and notification procedures in the event of data or system compromise. The credit union needs to conduct a sufficient analysis of the provider's security program, including how the provider uses available risk assessment tools and practices. Credit unions also should obtain copies of independent penetration tests run against the provider's system.

When assessing information security products, management should be aware that many products offer a combination of risk assessment features and can cover single or multiple operating systems. Several organizations provide independent assessment and certifications of the adequacy of computer security products (e.g., firewalls). While the underlying product may be certified, credit unions should realize that the manner in which the products are configured and ultimately used is an integral part of the products' effectiveness. If relying on the certification, credit unions should understand the certification process used by the organization certifying the security product. Other examples of items to consider in the risk assessment process include:

- *Identifying mission-critical information systems and determining the effectiveness of current information security programs.* For example, vulnerability might involve critical systems that are not reasonably isolated from the Internet and

external access via modem. Having up-to-date inventory listings of hardware and software, as well as system topologies, is important in this process.

- *Assessing the importance and sensitivity of information, and the likelihood of outside break-ins (e.g., by hackers) and insider misuse of information.* For example, if a member depositor list were made public, that disclosure could expose the credit union to reputational risk and the potential loss of deposits. Further, the credit union could be harmed if human resource data (e.g., salaries and personnel files) were made public. The assessment should identify systems that allow the transfer of funds, other assets, or sensitive data/confidential information, and review the appropriateness of access controls and other security policy settings.
- *Assessing the risks posed by electronic connections with business partners.* The other entity may have poor access controls that could potentially lead to an indirect compromise of the credit union's system. Another example involves vendors that may be allowed to access the credit union's system without proper security safeguards, such as firewalls. This could result in open access to critical information that the vendor may have "no need to know."
- *Determining legal implications and contingent liability concerns associated with any of the above.*For example, if hackers successfully access a credit union's system and use it to subsequently attack others, the credit union may be liable for damages incurred by the party that is attacked.

Potential Threats to Consider

Serious hackers, interested computer novices, dishonest vendors or competitors, disgruntled current or former employees, organized crime, or even agents of espionage pose a potential threat to a credit union's computer security. The Internet provides a wealth of information to credit unions and hackers alike on known security flaws in hardware and software. Using almost any search engine, average Internet users can quickly find information describing how to break into various systems by exploiting known security flaws and software bugs. Hackers also may breach security by misusing vulnerability assessment tools to probe network systems, then exploiting any identified weaknesses to gain unauthorized access to a system. Internal misuse of information systems remains an ever-present security threat.

Many break-ins or insider misuses of information occur due to poor security programs. Hackers often exploit well-known weaknesses and security defects in operating systems that have not been appropriately addressed by the credit union. Inadequate maintenance and improper system design may also allow hackers to exploit a security system. New security risks arise from evolving attack methods or newly detected holes and bugs in existing software and hardware. Also, new risks may be introduced as systems are altered or upgraded, or through the improper setup of available security-related tools. A credit union needs to stay abreast of new security threats and vulnerabilities. It is equally important to keep up to date on the latest security patches and version upgrades that are available to fix security flaws and bugs. Information security and relevant vendor Web sites contain much of this information.

Systems can be vulnerable to a variety of threats, including the misuse or theft of passwords. Hackers may use password-cracking programs to figure out poorly selected passwords.

The passwords may then be used to access other parts of the system. By monitoring network traffic, unauthorized users can easily steal unencrypted passwords. The theft of passwords is more difficult if they are encrypted. Employees or hackers may also attempt to compromise system administrator access (root access), tamper with critical files, read confidential e-mail, or initiate unauthorized e-mails or transactions.

Hackers may use "social engineering," a scheme using social techniques to obtain technical information required to access a system. A hacker may claim to be someone authorized to access the system such as an employee or a certain vendor or contractor. The hacker may then attempt to get a real employee to reveal user names or passwords, or even set up new computer accounts. Another threat involves the practice of "war dialing," in which hackers use a program that automatically dials telephone numbers and searches for modem lines that bypass network firewalls and other security measures. A few other common forms of system attack include:

- *Denial of service (system failure),* which is any action preventing a system from operating as intended. It may be the unauthorized destruction, modification, or delay of service. For example, in a "SYN Flood" attack, a system can be flooded with requests to establish a connection, leaving the system with more open connections than it can support. Then, legitimate users of the system being attacked are not allowed to connect until the open connections are closed or can time out.
- *Internet Protocol (IP) spoofing,* which allows an intruder via the Internet to effectively impersonate a local system's IP address in an attempt to gain access to that system. If other local systems perform

session authentication based on a connection's IP address, those systems may misinterpret incoming connections from the intruder as originating from a local trusted host and not require a password.

- *Trojan horses,* which are programs that contain additional (hidden) functions that usually allow malicious or unintended activities. A Trojan horse program generally performs unintended functions that may include replacing programs, or collecting, falsifying, or destroying data. Trojan horses can be attached to e-mails and may create a "back door" that allows unrestricted access to a system. The programs may automatically exclude logging and other information that would allow the intruder to be traced.
- *Viruses,* which are computer programs that may be embedded in other code and can self-replicate. Once active, they may take unwanted and unexpected actions that can result in either nondestructive or destructive outcomes in the host computer programs. The virus program may also move into multiple platforms, date files, or devices on a system and spread through multiple systems in a network. Virus programs may be contained in an e-mail attachment and become active when the attachment is opened.

CONCLUSION

It is important for credit unions to develop and implement appropriate information security programs. Whether systems are maintained in-house or by third-party vendors, appropriate

security controls and risk management techniques must be employed. A security program includes effective security policies and system architecture, which may be supported by the risk assessment tools and practices discussed in the Bulletin and appendix. Information security threats and vulnerabilities, as well as their countermeasures, will continue to evolve. As such, credit unions should have a proactive risk assessment process that identifies emerging threats and vulnerabilities to information systems.

A sound information security policy identifies prevention, detection, and response measures. The appendix provides more details on risk assessment tools and practices that may be used to improve information security programs. Preventive measures may include regularly using vulnerability assessment tools and conducting periodic penetration analyses. Intrusion detection tools can be effective in detecting potential intrusion or system misuse. Credit unions should also develop a response program to effectively handle any information security breaches that may occur.

RB 2014-03 Guidance on Indirect Automobile Lending

December 3, 2014

Introduction

Many traditional aspects of indirect automobile lending have changed in recent years. The captive finance companies of automobile manufacturers have made the auto lending business more difficult for credit unions. In an effort to compete for

automobile loans, many credit unions have tried to match the financial concessions of competitors by relaxing underwriting standards and cutting corners on processes and procedures. As a result some credit unions are operating in the highly competitive market with weak controls and lax loan underwriting programs, with predictable consequences. Further, it should also be noted that even credit unions with stronger programs are susceptible to diminishing collateral values and increased risk as loan terms are extended over longer periods.

Traditionally, the Department and credit unions have relied on a delinquency-based approach to evaluate automobile loan portfolios. This approach has served regulators and credit unions well in the past, but recent automobile financing trends require a more in-depth analysis when loan and collateral values are not correlated, vehicles are financed multiple times, or losses are deferred and embedded in loan balances.

This guidance reminds credit unions of certain aspects in the process that should be followed to prudently manage the risks associated with indirect loans. While there are benefits to a well-run indirect lending program, an improperly managed or loosely controlled program can quickly lead to unintended risk exposure. It takes proper planning and adequate controls and monitoring to make this type of program profitable and a productive activity for serving credit union members.

Background

Credit unions develop indirect automobile lending programs by establishing relationships with automobile dealers. Credit unions define the type of borrower and loan they will accept by providing dealers with underwriting and interest rate guidelines. In many cases, a dealership gathers credit information from prospective buyers, completes loan applications, and forwards the documents to the credit union for approval. Historically, automobile financing has been

perceived as a lower-risk form of lending, with risk spread among a large volume of smaller-balance, collateralized loans. Recent instances of weak indirect automobile lending programs, however, have indicated insufficient collateral values and marginal or deficient borrower repayment capacity, resulting in substantial financial consequences for the credit union.

Some evidence suggests that increased competition is negatively influencing indirect automobile lending programs. Heightened competition has prompted credit unions to offer lower interest rates, lengthen amortization periods, and scale down payment requirements. In some cases, competition has prompted credit unions to grant lending authority to the dealer in order to expedite the approval process for loans that fall within credit union-approved guidelines. Credit unions sometimes have extended their risk selection standards to enable them to finance lower credit quality accounts, often referred to as subprime loans. Today’s indirect automobile lending practices represent unique challenges to credit unions and the Department.

Types of Programs

In today’s marketplace, there are generally two types of automobile programs which are being utilized by credit unions. The first and most prevalent is a point of sale (indirect) relationship where the dealership provides loan application documentation, allowing the credit union to underwrite and decision the credit worthiness of the prospective borrower. If the prospective borrower qualifies for membership and an extension of credit, the borrower contracts directly with the dealership for the purchase of the automobile and subsequently the dealer assigns the resulting retail installment contract (indirect loan) to the credit union. Normally an indirect program is evidenced by a contractual relationship between the credit union and the participating dealership. The second program is less formal and is typically referred to as a

“dealer referral program”. As part of a referral program, the dealer may send the prospective borrowers directly to the credit union. The credit union may then qualify the borrowers for membership, and underwrite and decision the extension of credit utilizing the credit union’s internal loan standards. Regardless of the type of program, a credit union must be careful not to get lulled into a false sense of responsibility to approve loans. Ineffective underwriting and weak decision-making may result in high delinquencies and potentially larger charge-offs for the credit union. Under either program, if the loan losses become excessive, it can place the safety and soundness of the credit union and its future viability at risk.

Additional Scrutiny

Credit unions must recognize the additional risk inherent in today’s indirect lending and determine if these risks are acceptable and controllable given the credit union’s staff, financial condition, size, and level of net worth. Credit unions that engage in indirect lending in any significant way should have board-approved policies and procedures, as well as internal controls that identify, measure, monitor, and control these additional risks. The initial development of a sound indirect program includes a documented analysis of existing programs within the local marketplace. The analysis should include dealer reserve structures (i.e. flat fees, rate mark-up limitations, etc.); maximum loan maturities based on amounts financed; minimum credit scores allowed; maximum limits for “add-on” products; loan to value limits; and the basis for collateral valuation (NADA trade, retail, etc.). This analysis should provide the credit union with the basic framework to develop its indirect program limits. As part of the ongoing due diligence process for any indirect program, this type of analysis should continue on a regular basis throughout the life of the program. Another pertinent consideration during the implementation phase of the program

is whether the credit union's program will be geared toward franchise or non-franchise dealers, or a mixture of both. Generally speaking, non-franchise dealers may not possess the same level of financial stability as franchise dealers, and may not have the same quality of internal control processes in place. In some instances, this could elevate the potential for fraudulent transactions. Credit unions that engage in a small volume of indirect lending should have systems in place commensurate with their level of risk. Credit unions with existing indirect lending programs should carefully consider whether their program meets the following guidelines and should implement corrective measures for any area that falls short of these minimum standards.

The Department recognizes each credit union has its own individual risk profile and tolerance levels. However, as part of its ongoing supervisory monitoring processes, the Department will use certain criteria to identify credit unions that are potentially exposed to significant indirect lending risk. A credit union that has experienced rapid growth in indirect lending, has notable exposure to a particular credit risk category, or is approaching or exceeds the following supervisory criteria may be identified for further supervisory analysis to assess the nature and risk posed by the indirect lending program:

• Total reported indirect loans represent 250 percent or more of the credit union's net worth; or
• Total reported indirect loans represent 25 percent or more of the credit union's aggregate loan portfolio.

Field of Membership

As indicated by Section 122.253 of the Finance Code, credit unions may only make loans to its members, and, as such, borrowers in an indirect loan program must meet the field of membership requirements included in the credit union's bylaws and must become members of the credit union. Before

underwriting and making a decision on a potential extension of credit, a credit union should ensure the dealership provides adequate documentation to confirm whether the prospective borrower qualifies for membership. Evidence of the prospective borrower opening a credit union membership account must be retained, along with all other pertinent documentation. Further, a credit union must obtain all necessary information and follow all procedures for opening accounts as required under applicable law, including the Bank Secrecy Act, as amended by the USA PATRIOT Act, its implementing regulations, and any directives that may be issued. These requirements are in addition to the documents and disclosures required to be given or completed in conjunction with the extension of credit.

Risk Management

Prior to engaging in an indirect automobile lending program, the board and senior management of the credit union should ensure that proposed activities are consistent with the credit union’s overall business strategy and risk tolerances, and that the credit union has properly acknowledged and addressed critical business risk issues. These issues include the costs associated with attracting and retaining qualified personnel, investments in the technology necessary to manage a more complex portfolio, a clear origination strategy that allows for after-the-fact assessment of underwriting performance, and the establishment of appropriate feedback and control systems. The risk assessment process should extend beyond credit risk and appropriately incorporate operating, compliance, and legal risks. Finally, the planning process should set clear objectives for performance, including the identification and segmentation of target borrowers, and performance expectations and benchmarks for each segment and the portfolio as a whole. Credit unions establishing an indirect lending program should proceed slowly and cautiously into this activity to minimize the impact of unforeseen personnel, technology, or internal

control problems and to determine if initial profitability estimates are realistic and sustainable.

Staff Expertise

Indirect lending programs require specialized knowledge and skills that some credit unions may not possess. Account originations and collection strategies and techniques often differ from those employed for existing members; thus it may not be sufficient to have the same lending staff responsible for both indirect loans and other loans. Additionally, servicing and collecting indirect loans can be more labor intensive. If necessary, the credit union should implement programs to train staff. The board should ensure that staff possesses sufficient expertise to appropriately manage the risk in indirect lending and that staffing levels are adequate for the planned volume of indirect activity. Seasoning of staff and loans should be taken into account as performance is assessed over time.

Dealer Due Diligence Review Process

Credit unions should perform a thorough due diligence review of any participating dealer prior to purchasing an indirect loan. Credit unions should not accept indirect loans from dealers that do not meet their underwriting criteria, and should regularly review whether the prospective borrowers being offered by a dealership meet the established criteria. Deterioration in the quality of indirect loans or in the portfolio’s actual performance versus expectations requires a thorough reevaluation of the dealers who originated the loans, as well as reevaluation and adjustments of the credit union’s criteria for underwriting indirect loans and selecting dealers. Any such deterioration may also highlight the need to modify or terminate the correspondent relationship.

Loan Underwriting and Administration Procedures

After the indirect loan is purchased, loan administration procedures should provide for the diligent monitoring of loan performance and establish sound collection efforts. To minimize loan losses, successful indirect lenders have historically employed stronger collection efforts such as calling delinquent borrowers frequently, assigning more experienced collection personnel to seriously delinquent accounts, moving quickly to repossess collateral, and allowing few loan extensions. This aspect of indirect lending is labor intensive but critical to the program's success. To a large extent, the cost of such efforts can represent a tradeoff relative to future loss expectations when a credit union analyzes the profitability of indirect lending and assesses its appetite to expand or continue this line of business.

Credit unions should keep in mind that a large percentage of the borrowers in an indirect lending program may be new members to the credit union. These new members may not possess the same level of loyalty to the credit union as other segments of the existing membership. As a result, the collection efforts may need to be modified to begin contact earlier with the indirect loans than with other segments of the loan portfolio.

The credit union should be cautious about using different types of credit scores to qualify indirect borrowers than is used for existing borrowing members. The use of alternative credit scores, such as "auto enhanced," can place more emphasis on the repayment of certain loans in comparison to other outstanding debt obligations and the scoring model may provide a higher credit score than a standard credit bureau score. In addition to potentially increasing credit risk, the lack of consistency between the use of different types of credit scores can create discrepancies in the analysis of the

credit quality of the entire loan portfolio.

Loan Review and Monitoring

Once indirect loans are booked, credit unions must perform an ongoing analysis of these loans, not only on an aggregate basis but also for sub-categories. Monitoring performance for the entire indirect loan portfolio as well as by dealer is a critical factor to ensure the success of an indirect program. This monitoring may include the tracking of both early stage (i.e. 15 to 29 days; 30 to 59 days) and reportable delinquencies (60+ days), by dealer and credit score categories for each dealer. Additionally, the tracking of loan losses by dealer (broken down by credit risk categories) is a strong monitoring process. Credit unions should have information systems in place to segment and stratify their indirect portfolio (e.g., by dealer, loan-to-value, credit scores) and produce reports for the credit union to evaluate the performance of the indirect loan portfolio. In addition, comparison of the indirect segment relative to the credit union's total loan portfolio and other loan segments (i.e. direct auto loans) can provide the credit union valuable insight as to the performance trends of the indirect program. The review process should focus on whether performance meets expectations. Credit unions then need to consider the source and characteristics of indirect loans that do not meet expectations and make changes in their underwriting policies and loan administration procedures to restore performance to acceptable levels.

When evaluating actual performance against expectations, it is particularly important that the credit union review credit scoring, pricing and the adequacy of the Allowance for Loan and Lease Losses (ALLL). ALLL adequacy driven by the volume and severity of historical losses experienced during good economic times may have little relevance in an economic slowdown.

Reevaluation

Credit unions should periodically evaluate whether the indirect lending program has met profitability, risk, and performance goals. Whenever the program falls short of original objectives, an analysis should be performed to determine the cause and the program should be modified appropriately. If the program falls short of the credit union's expectations, the board and senior management should consider terminating it. Questions that the board and senior management need to ask may include:

• Have cost and revenue projections been met?
• Have projected loss estimates been accurate?
• Were the risks inherent to indirect lending properly identified, measured, monitored, and controlled?
• Has the program met the credit needs of the members that it was designed to address?

Compliance Considerations

Indirect automobile lending can also expose credit unions to compliance risk, particularly related to fair lending and unfair and deceptive practices. It is important to determine whether a credit union is considered a creditor and whether an agency relationship exists with the dealer. A creditor is defined by Regulation B. There can be multiple creditors in a single credit transaction. In indirect automobile lending there are usually at least two: the credit union and the dealer.

A credit union buying dealer paper (i.e., loans that have already been made) that did not influence and was not involved in the credit decision in any manner is not considered a creditor under Regulation B. However, a credit union that either influenced or was involved in the credit decision is considered a creditor and is subject to all fair lending regulations. It is also essential to determine the nature of

the relationship between a credit union and an automobile dealer. Credit unions are directly responsible for any discriminatory pricing or other discriminatory decisions made by a dealer acting as an agent of the credit union.

Credit unions should also monitor automobile lending programs for any evidence of unfair or deceptive conduct. Such conduct may arise through sales practices as well as through the financing and repossession process. Credit unions should consider incorporating a post audit process where the credit union contacts new borrowers (randomly, by dealership) to confirm a few key elements (i.e. term, rate, collateral including make and model, etc.) of the indirect loan to ensure there is no evidence of unfair or deceptive conduct.

Summary

Competition in the automobile lending market has increased significantly in recent years and is not expected to diminish in the near future. The results are thinning collateral and smaller net interest margins. The potential for heightened risk to credit unions in the areas of compliance, and safety and soundness, can be mitigated only through prudent lending policies and procedures, adequate internal controls, and strong oversight.
