OCC 98-38

OCC BULLETIN

Administrator of National Banks

Subject: Technology Risk Management: PC Banking

Description: Guidance for Bankers and Examiners

To: Chief Executive Officers and Chief Information Officers of all National Banks, General Managers of Federal Branches and Agencies, Deputy Comptrollers, Department and Division Heads, and Examining Personnel.

Purpose

The purpose of this bulletin is to provide guidance on how to identify, measure, monitor, and control risks arising from the use of retail personal computer banking ("PC banking"). It also sets forth the OCC's expectations of bank management and boards of directors when implementing and operating PC banking systems. All banks that provide or are actively planning to provide PC banking should follow these guidelines.

Summary of Key Points

- "PC banking" refers to computer hardware, software, and telecommunication systems that enable retail customers to access both specific account and general bank information on bank products and services through a personal computer (PC). The bank's network design and telecommunication links may include the use of private networks (e.g., direct dial-in using leased or dedicated telephone lines) or public networks (e.g., the Internet).

- PC banking can increase the level of direct interaction between a bank's customers and its internal networks and technology systems and can expand the connections between public networks, such as the Internet, and the bank's internal systems. Without proper internal controls, these situations may create significant security concerns.

- PC banking can expand the scope and reach of banking services, including the availability of services, the speed and volume of bank transactions, and the number and range of banking customers.

- In many cases, PC banking increases a bank's reliance on service providers and software vendors. Reliance on these third parties requires bank management to design appropriate risk controls for these relationships.

- PC banking primarily exposes a bank to transaction, strategic, reputation, and compliance risks, but may expose a bank to other risks as well. Management should ensure that banks and their service providers and software vendors have adequate controls in place to manage and monitor PC banking risks.

- To manage *transaction risk*, banks should:

  - Adopt effective and thoroughly tested security controls for PC banking that are integrated into a bank's overall security program through network and data access controls, user authentication, encryption, transaction verification, and virus protection controls;
  - Implement policies and controls according to the sensitivity and importance of data;
  - Establish effective risk monitoring processes, including security monitoring, performance monitoring, and audit/quality assurance reviews;
  - Include PC banking systems in bank contingency and business continuity plans; and
  - Identify special expertise, staffing needs, and training requirements.

- To manage *strategic risk*, banks should establish an effective planning process to implement and monitor PC banking systems. Management should ensure that PC banking is consistent with the bank's strategic and business plans and that adequate expertise and resources are available to operate and maintain their PC banking systems.

- To manage *reputation risk*, banks should adopt and test business continuity plans and establish customer service plans. Management also should establish and periodically test their communications plan and outreach strategy in order to respond promptly to adverse customer and media reaction caused by PC banking system problems or failures.

- To manage *compliance risk*, banks should monitor developments and changes in consumer and banking laws, regulations, and interpretive rulings and should take adequate measures to comply with them. Banks should consult with legal counsel to ensure that they have valid and enforceable contracts with their PC banking customers. Because the law is unsettled in many states on forming valid contracts through electronic media, banks should consider the risks that may arise as a result of relying on contracts entered into in this manner. An institution offering

Administrator of National Banks

PC banking in multiple states may face particular uncertainty when deciding which state laws apply to its operations. Similarly, institutions should assess whether they may be subjected to unexpected assertions of jurisdiction by courts, agencies and taxing authorities when they enter into new geographic, product, or service markets.

Scope and Reference

This bulletin focuses on the risk presented to banks by the use of PCS to initiate retail banking transactions. Retail customers also may use other devices, such as palmtop computers, kiosk technology, and screen phones, to conduct their banking activities. While the specific devices used may differ, many of the risks posed by them will be similar to the risks posed by PC banking. This guidance may be used to assist institutions in managing the risks that these technologies present.

While this guidance addresses information security controls used to safeguard confidential customer information, the OCC does not intend this guidance to provide comprehensive discussion of consumer privacy issues, such as electronic consumer disclosures, bank privacy policies, or customer information sharing.

This bulletin supplements the risk management process outlined in OCC-98-03, "Technology Risk Management." The Technology Risk Management bulletin describes the OCC's supervision by risk framework with respect to the risks posed by technology, sets forth the OCC's concerns regarding technology-related risks, and describes the risk management process associated with bank use of technology. This bulletin describes how that risk management process can be used to address the risks and controls specific to PC banking.

Introduction

PC banking presents opportunities and challenges. It provides a delivery channel that can expand a bank's geographic reach, increase customer convenience, and reduce transaction costs. In many ways, PC banking is similar to traditional payment, inquiry, and information processing systems. It differs, however, in that it allows customers to access information and conduct banking transactions from remote locations using personal computers, software applications, and telecommunication networks. PC banking services offer a new channel for banks to interact with their customers but may also introduce additional risks.

Administrator of National Banks

Although the current dollar volume of PC banking activity is small relative to the overall financial activity of most banks offering PC banking systems, some of the risks associated with these systems can be significant. PC banking can substantially increase customer access to a bank's internal systems via public networks, such as the Internet, and can introduce a number of security issues. These security issues may pose transaction and reputation risk even when the volume of PC banking activity is relatively small.

In addition to expanding a bank's customer base, a bank also may find that its PC banking customers have different expectations than traditional bank customers regarding the availability and convenience of services. For example, customers who rely on PC banking services may have greater intolerance for any situation in which the system is not readily available and does not provide accurate and current information.

In many cases, PC banking will increase a bank's reliance on service providers and software vendors to design, implement, and manage PC banking systems. The degree to which banks choose to operate their PC banking systems through service providers and software vendors will affect the extent of the bank's involvement in actual systems design, planning, and other day-to-day operational and monitoring issues. For example, banks that outsource all of these functions will have less "hands on" involvement in detecting unauthorized intrusions into a bank's PC banking system, than those banks that perform some or all of their security and operational functions in-house. As with any outsourced product or service, reliance on service providers and software vendors for PC banking will require sound risk management practices.

Legislatures and regulatory agencies are reviewing and modifying laws and regulations that may affect PC banking and bank compliance. Banks must ensure that they monitor these developments and comply with statutory and regulatory changes in a timely manner.

PC Banking Risks and Controls

PC banking systems primarily expose banks to transaction, strategic, reputation, and compliance risk, but may expose a bank to other risks as well. For example, PC banking systems may present credit risk if a bank offers lending services over the Internet. "Know your customer" considerations in this context may require the use of different identification, authentication, and transaction verification methods than those used with traditional delivery channels. Liquidity, interest rate, market, price, and foreign exchange risks may result from poor data integrity or unreliable systems. The OCC expects banks to carefully consider the full range of these and other issues and the potential risks that they may pose in deciding whether to adopt a PC banking system or to renovate an existing one.

PC banking risks should be managed as part of a bank's overall risk management process. As described more fully in OC-98-03, "Technology Risk Management," banks should use a rigorous analytic process to identify, measure, monitor, and control risks. The quantity of risk assumed should be consistent with the bank's overall risk tolerance and must not exceed the bank's ability to manage and control its risks. Management and bank staff are expected to have the knowledge and skills necessary to understand and effectively manage their PC banking-related risks. Examiners will evaluate PC banking risk by reviewing technology plans, policies, controls, monitoring techniques, and relevant compliance issues. In addition, the OCC may evaluate system performance and the effectiveness of specific controls.

If a bank decides to use service providers or software vendors to provide PC banking services, management should exercise appropriate due diligence in evaluating their reputation, financial status, and viability. This will help ensure that the service providers and software vendors can perform as promised and that they are capable of keeping abreast of new or changing technology. When contracting for PC banking services, management should carefully consider how it intends to use third parties to design, implement, and support all or part of its PC banking systems. Bank management should ensure that adequate controls are in place to monitor performance levels and to swiftly respond to any problem or emergency. This could be accomplished, for example, by providing specific performance benchmarks and reporting requirements in service provider and software vendor agreements with respect to the items discussed in this bulletin.

A primary concern for bank management when outsourcing is maintaining control over the services and products provided by third parties. For example, when negotiating contracts, management should confirm that responsibilities and accountability are clearly defined for each party. Management should ensure that the bank can exercise the control necessary to properly manage the products or services. Control items should include, but not be limited to, the bank's ability to perform audits or to obtain from the service provider or software vendor independent internal control audits. Bank management should establish controls that allow the bank to confirm third party recovery plans, review their financial condition, and establish data ownership with the third party. Management should establish its rights, to the extent possible, in the event a third party fails to perform under the contract or fails altogether. The bank also should consider the conditions under which it can terminate or change service providers or software vendors without incurring substantial liability in the event plans change or performance standards are not met.

Regardless of how a system is developed or operated, the OCC's expectation is for banks to effectively manage their PC banking risk. Controls should take into account the level of risk posed to the institution and should be adopted by the party in the best position to control the risks. In some instances, that party may be an outside vendor or service provider. In practice, the controls necessary to effectively manage risk will differ depending on the degree of risk posed and how the PC banking system is designed and operated. Transaction, strategic, reputation, and compliance risks are discussed separately below.

Transaction Risk

Transaction risk is the most common source of risk arising from PC banking. It results from weaknesses in design, implementation, and monitoring. PC banking systems should be safe and secure. Transactions should be accurate and legally enforceable, and the records of these transactions should be reliable and accessible. Security controls are critical because they can help preserve system performance and mitigate the risk of exposure to unauthorized access and intrusions that can lead to poor performance, inaccurate data, or disclosure of confidential, customer or bank, information. Similarly, incompatible hardware and software and capacity constraints can affect PC banking system availability and reliability. Transaction risk also may increase when banks, exploring PC banking options, find that they are unfamiliar with certain types of new technology. Bank management may lack the necessary expertise or resources to design and implement a secure and reliable system. As a result, banks may seek to outsource all or part of their PC banking systems to meet expertise needs. Outsourcing may also occur to gain operating efficiencies or to achieve a competitive advantage. Whatever the rationale, transaction risk can arise from outsourcing activity and banks must ensure that they appropriately manage these new or expanded relationships.

Information security is critical to the safe and sound operation of a PC banking system. Connections with public networks, such as the Internet, can expose a bank to significant security challenges, including unauthorized users and intrusions, system failures, access and data privacy issues, and computer viruses. PC banking also greatly increases the level of direct interaction between bank customers and internal bank technology systems. These factors increase a bank's potential transaction risk exposure. Effective security and monitoring are critical to controlling transaction risk.

When assessing transaction risk, examiners will evaluate PC banking systems to determine the adequacy of operating policies and procedures, internal controls, and system monitoring. Examiners also will assess the controls used by banks to manage transaction risk, including security, business continuity and contingency plans, and management and staff expertise and training. Where these functions are performed by service providers or software vendors, examiners will evaluate whether bank management has assessed its risk exposure and established the necessary controls to ensure that the third parties are performing these functions properly.

Control: Security. PC banking systems require effective and reliable controls to maintain data integrity, ensure customer privacy, and protect the bank's computer and telecommunications systems from unauthorized intrusions, misuse, or fraud. Risk management controls for PC banking should be incorporated into a bank's overall security program. A security program should provide "end-to-end"[1] security controls for critical data and critical facilities.

Management should conduct periodic security risk assessments 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 PC 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 a bank's security program, management should ensure that an objective and qualified source reviews and tests the controls to ensure their effectiveness.

A bank's overall security program should include a security policy, an awareness program, and security controls. These elements are not unique to PC banking, but rather are discussed here to emphasize the importance of a sound program in managing risks that may arise from the use of electronic banking systems.

[1] "End-to-end" security provides bank-wide implementation of physical and data security controls to protect a bank's critical information, human resources, and physical assets from internal or external intrusion or compromise.

Administrator of National Banks

- Security Policy and Awareness Programs. A bank's security policy should establish clear expectations and a commitment to an ongoing program. The security program should set forth policies, procedures and controls to safeguard the bank's information, define individual responsibilities, and describe enforcement and disciplinary actions for non-compliance. Management also should establish specific reporting requirements for security breaches.[2] A security awareness program should be adopted to give users a clear understanding of the procedures and controls necessary for a secure environment. This security awareness program should reinforce the bank's security policy and program and may include, for example, instructions regarding password protection, Internet security procedures, user responsibilities, and employee disciplinary actions.

- Security Controls. Management should develop security controls that govern network and data access, user authentication, transaction verification, and virus protection.

  Network and Data Access Controls. Access controls allow verification and enforcement of a user's authorized right to access a bank network, applications, and data. The bank should identify internal and external users of a bank's networks or other computer systems. Access controls should restrict unauthorized individuals from entering critical facilities, retrieving confidential information, or allowing access to bank software applications and operating systems.

  User Authentication. Authentication is the process of determining whether PC banking system users are whom they claim to be. In general, banks should authenticate the identity of PC banking customers when customers access personal account information or engage in on-line transactions for products or services. Management should select reliable and accurate authentication processes based on the potential threats and vulnerabilities that the PC banking system poses, the bank's risk tolerance, and the bank's ability to manage those risks. Strong authentication generally combines at least two of the following factors: (1) something a customer knows (e.g., passwords, personal identification numbers (PINs)), (2) something the customer has (e.g., key, ATM card, identification card), and (3) something the customer is (e.g., finger prints). While more advanced technologies such as random password generators, digital signatures and forms of biometrics may be used to achieve even stronger

[2] For additional guidance, see OCC Advisory Letter 97-9, "Reporting Computer Related Crimes."

authentication, we recognize that many of those techniques are not yet widely used and can be costly.

Today, most private PC banking systems (e.g., those that use direct dial-in using leased or dedicated telephone lines) use single passwords or PINs to verify a customer's identity ("single password systems"). To date, the OCC is unaware of any significant losses suffered by a bank resulting from the compromise of a customer's password. Despite this, most experts agree that single password systems do not now and will not in the future provide totally adequate user authentication. A single password can be too easily compromised by eavesdropping on a conversation, gaining access to a customer's computer, installing a keystroke capturing program on a PC, or simply asking a customer for their password while posing as a bank official. Once compromised, an unauthorized user could have unrestricted access to a customer's accounts, and potentially access to a bank's internal systems.

Security and risk management concerns related to specific PC banking systems may require stronger authentication methods than those provided by single password systems. As Internet fraud, computer crimes, and other security concerns increase, single password authentication may quickly become outmoded. For example, where banks implement PC banking systems that rely on the Internet, security concerns increase because information, including passwords and PINs, move through multiple external networks as the data is processed. A single password without an accompanying card, key or combination of passwords, generally will not provide sufficient authentication of bank customers. Regardless of the authentication processes selected, banks should review and periodically test the effectiveness of those processes through penetration testing and other monitoring methods. They also should consider whether new or developing industry standards may affect the bank's existing use of authentication devices and processes.

In some circumstances, security and access concerns may require little or no authentication. For example, when a user seeks access to information only from a bank's Internet web page, passwords and other authentication techniques typically are not necessary.

Banks should use a combination of access, authentication and other security controls to create a secure and confidential PC banking environment. These generally include passwords, firewalls, and encryption. Each is discussed below.

- Passwords. Banks should assign passwords or PINs to users to control access to PC banking systems and should help to ensure the integrity of passwords by providing instruction on their proper use and protection. Specifically, management should consider the following password protection practices:

    - Minimum character length for passwords;
    - Use of alphanumeric passwords;
    - Periodic changes in passwords through automatic expiration;
    - Procedures for resetting user passwords and identification;
    - Session controls that ensure automatic log-off for inactivity and excessive failed access attempts;
    - Prohibition of unencrypted, or clear text, password storage;
    - Encryption of passwords or PINs during transmission; and
    - Disallowance of automatic password save features.

- Firewalls. Firewalls combine hardware and software to block unwanted communications into and out of a bank's network, while allowing acceptable communications to pass. Types of firewalls and their configurations vary considerably, ranging from simple routing devices to complex multiple firewall configurations. Management should use firewalls to protect the bank's internal network and to protect all connection points between the internal network and external networks, such as the Internet. Management should position firewalls based on the desired level of security as dictated by the bank's risk assessment and data classification efforts (see data classification discussion, below). Because firewall design and implementation can be complex, management should obtain certification of the effectiveness of its firewalls from an objective qualified internal or external source with adequate security expertise. Periodic review and testing of firewalls should be conducted as needed as part of the bank's security monitoring efforts. If firewalls are designed and implemented by service providers and software vendors, the bank should periodically assure that vendors have internally or externally tested firewalls and that they operate properly.

- Encryption. Encryption transforms data into an unreadable format.

> Management should choose levels and types of encryption based on the sensitivity of data or information being transmitted. Encryption should be used when transmitting sensitive or critical data, such as confidential customer information, over public networks, such as the Internet. 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. Key confidentiality is achieved through sound key management practices. Data sensitivity and vulnerability to threat or compromise are important factors in management's decision-making regarding the use and strength of encryption. Management should protect encryption keys under the bank's control and they should educate customers about the importance of keeping private keys secret. Management should require customers to contact the bank if a private key is compromised.[3]

Transaction Verification. PC banking agreements should define the procedures for valid and authentic electronic communications between the bank and its customers. The agreements should specify that the parties intend to be bound by communications that comply with these procedures. Management also should verify and maintain audit trails of parties who initiate transactions. Audit trails enable a bank to verify specific transactions and can provide proof of transactions to avoid claims of repudiation by bank customers.

Virus Protection. Virus protection is an important security control in operating any

[3] For purposes of this bulletin, protection of a customer's private key refers to the key used in either private (symmetric) crypto systems and public (asymmetric) crypto systems. Asymmetric crypto systems use two keys, private and public, while symmetric systems require only one private, or secret, key to encrypt and decrypt data. Although different, both encryption techniques require that the secret or private key be strictly controlled to maintain the integrity of the crypto system.

computer system.[4] Viruses can cause significant damage to the integrity of a bank's computer network, applications, and data files. They also can result in unreliable service. Any time a connection is made to an external or internal network, an opportunity for infection from computer viruses exists. Management should establish a bank-wide detection and prevention program to reduce the likelihood of computer viruses. This should include end-user policies, training and awareness programs, virus detection tools, and enforcement procedures.

Control: Data Classification. Management should consider classifying, or "categorizing", data according to its sensitivity and importance. Critical applications or information, if altered or inaccessible, can seriously affect the bank's ability to operate and may result in significant loss. Therefore, effective security processes are required to safeguard critical applications and data. Data classification considerations may include: establishing data ownership; determining vulnerability to data loss, destruction, or disclosure; and identifying the impact these adverse events may have on the bank's operations, reputation, and profitability.

Control: Monitoring. Monitoring is essential for effective PC banking risk management. Data generated by monitoring techniques allow management to measure performance and assess the effectiveness of security controls. Management should ensure that monitoring is consistent with applicable laws and regulations governing access to or use of sensitive or confidential information.

- Security Monitoring. Management should place 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 a bank's security policy, staff should report security breaches promptly to appropriate management and external officials. While many ways exist to monitor security, management should 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,

[4] Firewalls do not detect viruses with any degree of accuracy because virus detection software cannot scan messages or codes that are compressed or encrypted. The message must be decompressed, scanned, recompressed and then sent through the firewall to be delivered. This can seriously affect the response time of the network.

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 do not guarantee that firewalls will prevent all types of attacks. Management should use penetration testing techniques to evaluate the effectiveness of security controls and should ensure that testing is conducted by an objective, qualified, internal or external source at least once a year or whenever substantial changes are made to the PC banking security systems. If a bank's PC banking services are provided by an outside vendor or service provider, management should ensure that the contracted company or entity has performed adequate penetration testing and provided management with the results of the testing.

Intrusion Detection. Transaction and audit logs can be produced through firewall technology and can be used to detect network activity or intrusions. The reports that are produced are often voluminous and difficult to review, resulting in the possibility that urgent security issues may be overlooked or trends may go unnoticed by management. Automated intrusion detection devices are available that monitor network traffic on a real-time basis. These systems can log suspicious activity and the information can be used to notify security administrators, or even terminate suspicious network connections. Management should consider real time intrusion detection systems where transaction activity cannot be effectively monitored through manual processes or systems.

Intrusion detection tools also enable management to maintain an incident database for trend analysis of network intrusions and attack attempts. Information compiled in this manner can be used to compare network traffic against prescribed security policies and system settings. For example, if the bank's security policy prohibits File Transfer Protocol (FTP) and TELNET[5] transmissions, this monitoring process would check for instances in which firewalls may have allowed these transmissions to pass.

[5] FTP and TELNET are Internet communication standards that are used for transferring files from one computer to another and for enabling users to establish remote terminal connections by interacting with a remote time sharing system, respectively.

Following the detection of an unauthorized act or user, management should, as part of its security policy, 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 to the cause and scope of the breach. They also should discuss the extent of damage or disclosure of information, and what risks, including legal liability, the bank may incur. If monitoring processes are outsourced, similar notification to bank management should occur. Bank response activities should include communications with customers, and, where appropriate, law enforcement agencies, regulatory agencies, and the media.

- Performance Monitoring. Management should select several key performance indicators to determine whether the PC banking system is working as planned. Indicators may include such items as system response times, system availability, types of customer inquiries, problem resolution, traffic volume, and customer profiles. Performance monitoring reports can contribute significantly to identifying system inefficiencies, addressing performance problems, and estimating capacity needs.

- Audit/Quality Assurance. An objective review of PC banking systems should identify and quantify risk, and detect possible weaknesses in the bank's risk management system as it pertains to PC banking. Management may rely on internal audit, external audit, or other qualified professional sources to conduct this review. The objective review should critique the PC banking system design, assess the adequacy of internal controls, and ensure that appropriate policies, procedures and standards are developed and practiced. If the bank lacks internal expertise, management should use other qualified professionals, such as management consultants or CPA firms, to provide an independent review. If auditors are used, they should consult with management during the planning process to ensure that the PC banking system can be thoroughly audited in a cost-effective manner. If most or all of a bank's services are provided by service providers or software vendors, management should ensure that the service providers and software vendors have performed similar reviews of the type described here, and management should receive results of those reviews.

Control: Contingency Planning/Business Continuity. Management should incorporate PC banking systems into the bank's overall contingency planning and business continuity efforts.

Similar to other processes and applications, the bank's recovery plan for PC banking should be based on a business impact analysis. This analysis should evaluate business applications and processes to determine their importance and establish a prioritized order of business resumption designed to recover the most critical functions and systems first. Management should review and test interrelated components of the PC banking system with both internal and external systems to ensure that the bank's systems can successfully execute recovery plans.

Control: Expertise. Management should identify special staffing and training needs for personnel involved in system development, operation, and customer support. They also should determine how they will allocate resources to hire and train employees to run and support the PC banking system. Banks, service providers, and software vendors that heavily rely on technology should devote sufficient staff and resources to ensure that they can run the PC banking system and address any related security concerns. Insufficient training and inadequate expertise can result in productivity loss, operational problems, and unfulfilled customer expectations. Staffing plans should address how systems will be supported if a critical person leaves or if the usage of the system exceeds expectations. In addition, management should periodically assess training needs in light of technological and personnel changes that may occur. Where internal expertise is unavailable, management should obtain appropriate external technical support to help plan, operate, and monitor the system.

Strategic Risk

Strategic risk arises when management fails to adequately plan for PC banking systems, either in-house, or through service providers and software vendors. When implementing PC banking systems, effective planning helps a bank maintain a level of risk that is manageable and within its risk tolerance. Planning activities should establish strategic goals, and identify and quantify, to the extent possible, PC banking risks. Management should assess the impact PC banking may have on operations and the bank's financial condition should the system fail to perform as planned or fail completely. For example, planning should include potential issues such as internal and/or vendor incompatibility, system capacity needs, customer service responsibilities and ongoing maintenance costs. Management should have a general understanding of the risks associated with PC banking and should supplement their technical knowledge, as needed, with expertise provided by business managers, technology staff, and outside experts. Because industry standards are evolving, management should seek to develop systems that can, without excessive cost or burden, accommodate changes over time.

The OCC will evaluate a bank's effectiveness in controlling strategic risk related to PC banking by assessing whether the bank adequately plans for, implements, and monitors its PC banking system. For example, the system needs to be compatible with the bank's strategic goals, business tactics, and overall risk tolerance. The extent and scope of this planning may differ depending on whether the planning occurs primarily in-house or through service providers and software vendors, and depending on the complexity of the PC banking system.

Reputation Risk

Reputation risk may arise if PC banking systems are unreliable, if performance or data integrity is flawed, or if private customer information is compromised. Such events may lead to adverse customer and media reaction. Reputation risk also may arise if the bank fails to provide adequate disclosure of information or fails to resolve customer problems associated with the use of PC banking systems.

Management should be prepared to respond to operational failures or unauthorized intrusions that may increase the bank's exposure to reputation risk. They also should establish and periodically test a communications plan and outreach strategy for prompt response to adverse customer and media reaction caused by PC banking system failures or problems. Banks should provide customer support to supplement their PC banking services and to reduce exposure to reputation risk. Customer service affords a bank the opportunity to minimize the negative impact that occasional system failures or performance problems may have on a bank's reputation by restoring customer trust and satisfaction.

Compliance Risk

Compliance risk arises in PC banking when a bank violates or fails to conform with laws, rules, regulations, prescribed practices, or ethical standards. It also arises in situations where the manner and extent to which current laws or regulations apply to PC banking transactions is not clear. For example, because some federal consumer protection rules applicable to national banks, including disclosure and notice rules, assume the presence of a paper-based media, the application of those rules to electronic commerce is uncertain.[6]

[6] Refer to the Federal Financial Institutions Examination Council Press Release, *Interagency Council Issues Guidance on Electronic Financial Services and Consumer Compliance,* dated July 15, 1998, for additional detail.

Banks should consult with legal counsel to ensure that valid and enforceable contracts exist with their PC banking customers. To date, banks have offered their PC banking products only to pre-existing customers or have established new customer relationships in traditional ways. For example, banks send out, and request customers to sign and return, signature cards before offering PC banking to these new customers. If established in this manner, a traditional customer/bank contract exists. However, because the law in many states is unsettled on forming valid contacts via electronic media, banks should consider the risks that may arise as a result of relying on contracts entered into solely through electronic communications. Similarly, banks should carefully review the relevant state law on signature requirements that may apply to transactions performed via PC banking systems. In many states, for example, it is not clear whether traditional document requirements will be satisfied by electronic documents, or whether various forms of electronic authentication will be needed to satisfy the requirements for a signature.

Because some consumer regulations require that specific data be collected and retained, banks offering PC banking services must ensure that PC banking systems are capable of collecting and retaining the necessary data. For example, banks must ensure that their PC banking systems are designed and operated in a manner that complies with the Bank Secrecy Act, which requires that banks take steps to verify the identity of customers engaging in certain transactions, record and report data on those transactions, implement anti-money-laundering programs, and report suspicious transactions. Banks offering PC banking also must be cognizant of applicable privacy rules that may restrict their ability to share information that they obtain with third parties.

PC banking may cause the bank to enter new geographic or product markets[7] that could subject the bank to unexpected assertions of jurisdiction by courts, agencies and taxing authorities. For example, the law is currently unsettled on whether a firm that is offering products and services over the Internet subjects itself to the procedural and substantive jurisdiction of any state where customers or potential customers reside even if the firm has no actual physical presence in the state. Thus, a bank offering PC banking in multiple states may face uncertainty over which set of state substantive laws (e.g., consumer protection, licensing or franchise tax laws) will apply to its operations in various states.

[7] By offering PC banking services, banks may enable customers to access, via Internet links, other third party services or products. Banks should analyze the risks presented by these arrangements, particularly compliance and reputation risks. For example, banks should consider the need for disclosures to make clear when non-banking services are being offered by third party vendors and not by the bank and that the bank is not responsible for such services.

As state and federal governments consider new laws, rules, and interpretations that may affect PC banking systems, management should monitor these developments at the federal level and in the states in which they offer PC banking systems. Once final rulings are made, bank management should ensure that the bank is in compliance with these law(s) and regulations.

Responsible Office

Questions regarding this banking circular or the information it contains should be directed to the Bank Technology Unit, (202) 874-2340 or via E-mail: Norine.Richards@occ.treas.gov.

____

Emory W. Rushton
Senior Deputy Comptroller for
Bank Supervision Policy