RESCINDED

#70

Office of Thrift Supervision
Department of the Treasury

John F. Downey
Executive Director, Supervision

1700 G Street, N.W., Washington, D.C. 20552

Rescinded by CEO Memo 204

June 23, 1997

MEMORANDUM FOR: Chief Executive Officers

FROM: John Downey
Executive Director, Supervision

SUBJECT: Statement on Retail On-Line Personal Computer Banking

The Office of Thrift Supervision (OTS) recognizes that retail on-line personal computer (PC) banking offers opportunities for financial institutions to enhance customer relationships and improve competitive positions. As financial institutions begin using technological innovations to efficiently provide products and services to their customers, the risks must be considered and appropriate controls put in place. OTS is issuing this statement to alert the Board of Directors and management to some of the risks and concerns of retail on-line PC banking. I encourage you to share the information with your Board of Directors and appropriate staff.

OTS wants to stay abreast of industry trends with respect to emerging technology. Financial institutions engaging in, or contemplating PC banking, should inform and consult with their OTS Regional Office as they consider and implement such programs. Questions concerning this statement should be directed to Paul Reymann, Policy Analyst, Supervision Policy, on (202) 906-5645, Paul Glenn, Special Counsel, on (202) 906-6203, or Paley Pang, Manager and Regional Information Systems Examiner, on (415) 616-1554.

Attachment

Office of Thrift Supervision

Statement on Retail On-Line PC Banking

BACKGROUND

New technologies make it possible for financial institutions to offer a wide range of innovative products and services via the personal computer. Retail on-line personal computer (PC) banking exemplifies an emerging delivery channel for retail banking services made possible by technology.

PC banking involves the use of a PC to interact with a financial institution. Customers can use their PC and modem to contact the financial institution via dial-up telephone lines connected directly to the institution, third-party vendors, or the Internet[1]. Potential applications of this technology include, but are not limited to, providing on-line account inquiries, bill payments, intra-bank funds transfers, credit card and loan applications, insurance services, brokerage services, digital images of checks, and advertising financial products and services on the World Wide Web[2].

RISKS AND CONTROLS

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

* Review the implications of PC banking on the institution's strategic plan;
* Evaluate customer expectations and demands;
* Evaluate internal and external expertise and resource requirements to support the PC banking system;
* Assess the risks and required controls, particularly those related to system security; and
* Develop effective policies and procedures that cover the program.

PC banking activities involve a wide range of potential risks. Some of these are unique to this new delivery channel, while others represent general concerns that are common to traditional banking practices. When implementing a PC banking program, as with any new program, management must ensure that unique areas are identified and addressed. Traditional risk management techniques should also be expanded to incorporate new delivery channels and devices. For example, new computer hardware and software may be needed to control security threats, while existing audit procedures will require expansion to incorporate the new system.

[1]The Internet is a global system of interconnected computer networks that transmit data over telephone lines, television cable, and satellite links. The Internet was designed to disseminate information quickly to any party on the interconnected network. The Internet has no security administrator, and no single entity exercises control.

[2]The World Wide Web is a portion of the Internet which supports multimedia applications and consists of richly formatted hypertext "pages" which can be accessed with the use of special software, known as a "browser."

Generally, PC Banking related risks can be categorized as Strategic, Legal/Regulatory, and Operational. Within these general risk areas, there are several concerns that are unique to PC banking. Each of the general risk areas are explored more fully below, along with examples of compensating controls.

Strategic Risk

Strategic risk exists in the business decisions that a financial institution faces when new products or services are introduced. Four specific concerns that each institution should address for any new product or service are: (1) the development of a business plan which justifies the program; (2) availability of sufficient resources to support the program; (3) whether to outsource certain functions or perform them in-house; and (4) staying abreast of technological developments.

Business Plan

The decision to offer a PC banking program should be justified by a positive business plan. In developing the business plan, management should:

- *Conduct Research and Consult with Experts* **-** Management should consult with qualified technological, legal, economic, audit, regulatory, and other experts to evaluate pertinent issues.

- *Perform Strategic Technology Planning* - Technology planning is a part of the strategic planning process. The financial institution should clearly define its goals and objectives in this area and allocate sufficient resources.

- *Establish Goals and Monitor Performance*- Performance goals measure the success of the PC banking program. The program should be reevaluated periodically in light of strategic plans, customer satisfaction, and new technologies.

Internal and External Resources

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

- *Provide Adequate Training* - The institution's staff should be properly trained to implement the program. Specifically, they should be educated on new security procedures and control practices. Qualifications of external personnel should be evaluated prior to contracting with the vendor.

- *Provide Adequate Support Staff* - Support staff (e.g., call center staff and customer service representatives) should be kept informed of any changes or updates to the program. Additional personnel may be needed to address an increased volume of customer inquiries.

- *Maintain Software Updates* - Software changes require administrative controls. The institution may have to rely on customers to install software updates and accommodate those who are unable or unwilling to upgrade. Multiple software versions may have to be supported.

- *Establish Adequate Insurance Coverage* - Insurance providers should be consulted to confirm adequate coverage for PC banking activities.

Outsourcing Arrangements

Outsourcing arrangements are commonly used for many aspects of PC banking programs. However, such arrangements must be properly initiated, documented, and managed. Insufficient control over a vendor can result in potential liability and embarrassment to a financial institution. When an institution plans to outsource part or all of its PC banking program, they should:

- *Perform Due Diligence on Vendors* - Select only vendors who are knowledgeable of the emerging technology. Many institutions will partner with service bureaus and software vendors to develop, offer, and distribute PC banking services. Management should consider the vendor's financial condition and ability to provide ongoing services.

- *Audit Performance* - The performance of the vendor should be monitored and compared to the provisions of the contract.

- *Establish Back-up Arrangements* - The possible inability of a vendor to fulfill its obligation should be considered by management. The degree of difficulty and cost to obtain a replacement should determine the extent to which back-up arrangements are considered.

Technological Developments

The dynamic nature of technology makes it incumbent on financial institutions to maintain secure systems that meet customer needs. An institution's information technology plan should include consideration of future system upgrades as more sophisticated security techniques and user options are developed. To help ensure a secure PC banking program that continues to meet

customer needs, management should:

- *Monitor New Developments* - Plan for periodic evaluations of new technologies in hardware and software. Management should evaluate new products, services, and vendors against strategic plans and in light of the aforementioned risks.

- *Budget for Technology Upgrades* - Appropriate consideration should be given to the costs of technological upgrades to maintain appropriate security and adapt to customer expectations.

Legal/Regulatory Risk

Legal/Regulatory risk arises from the uncertainty of how the electronic environment will affect legal framework, jurisdiction, and regulatory compliance. Countermeasures generally consist of effective policies and procedures and comprehensive consumer disclosures.

Legal Framework

Many basic legal questions complicate electronic commerce and banking activities. The applicability of existing laws in an electronic environment is uncertain in many cases and financial institutions must exercise caution when addressing legal issues related to PC banking. Until more stability can be provided through answers to many of these legal questions, management should consider:

- *Detailed Contracts* - When certain functions of a PC banking program are outsourced, detailed contracts are used to define the roles and responsibilities of the financial institution and vendors. Contracts should include delineations of authority, responsibility, and accountability; provide protective covenants; and address confidentiality, ownership of bank records, and safety of customer assets. OTS Thrift Bulletin (TB) 44, Interagency Statement on EDP Service Contracts, and TB 46, Contracting for Data Processing Services or Systems offer additional guidance related to contracting for EDP services.

- *Digital Signatures* - Digital signatures represent a means to authenticate the parties to a transaction. Digital signatures are created with the use of encryption technology; however, they are not universally accepted and recognized. Management should explore the use of digital signatures and monitor legal developments in this area.

- *Comprehensive Disclosures* - Management should ensure that customers are fully informed of the risks associated with their participation in a PC banking program. Consumer disclosures should explain the circumstances under which their account data may be at risk and the security methods employed by the financial institution. Customers must be informed of their rights and responsibilities in the event of unauthorized access.

Jurisdiction

Jurisdiction is a complex issue in an electronic environment. The question of which state or federal, or international laws apply to a particular transaction remains unanswered. Financial institutions must consider the implications of conducting business with customers in different states and countries. Management should:

- *Consult with legal counsel to identify and address relevant legal issues.*

- *Identify the institution s trade area and develop a policy for responding to requests from parties who are not within the defined trade area.*

Regulatory Compliance

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

- *Update Policies and Procedures* - Existing policies and procedures should be modified as needed to incorporate the PC banking program.

- *Consult with the OTS Regional Office* - Financial institutions should consult with their OTS Regional Office as they consider and implement PC banking programs.

- *Expand Internal and External Audit* - Programs to monitor compliance with regulatory requirements should be expanded to include electronic delivery channels.

Operational Risk

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

Security

Security is the paramount issue, since access via dial-up telephone and the Internet both represent an opening of the computer system to outside and potentially unauthorized users. Remote banking activities may also be conducted through other interactive devices, such as automated teller machines, telephones, and televisions. Although the devices and distribution channels are different, the risk and control issues delineated in this document are generally applicable, regardless of the type of access device or distribution channel.

System security requires implementation of proper controls to guard against unauthorized access to the financial institution's networks, systems, and databases. Management should control user access to prevent a security compromise of internal systems. Customer data must be protected from unauthorized access or alteration during transmission over public networks. Management should develop methods to maintain confidentiality, ensure the intended person receives accurate information, and prevent eavesdropping by others. In addition, to ensure non-repudiation, undeniable proof of participation by both the sender and the receiver in a transaction must be created. Controls that management could implement include:

- *Authorization* - Authorization involves the pre-determination of permissible activities. Management should ensure that customers have access only to their own accounts and perform only authorized functions.

- *Access Controls* - Traditional access controls, such as user identification, passwords, and personal identification numbers (PINs)[3], should be implemented for PC banking customers. However, since the effectiveness of these controls is greatly influenced by the customer, management should take all possible steps to educate the customer in this area.

- *Authentication* - Authentication is used to verify and recognize the identity of parties to a transaction. Financial institutions may communicate with customers they never physically meet resulting in opportunities for misrepresentation. Digital certificates are being explored as methods of authentication in the PC banking environment. Authentication is the primary component of non-repudiation.

- *Secure Data Storage* - Confidential information or highly sensitive data should be stored securely. Management should consider storing sensitive data in encrypted form and implementing stringent access controls.

[3]To improve security,PINs should be unique, non-sequential, and not easily identifiable.

- *Encryption* - Encryption technology disguises information to hide its meaning and enhances confidentiality by restricting information access to only intended users. Encryption-based methods can also be used to verify message authenticity and accuracy. Information is encrypted and decrypted with a cipher and key using specialized computer hardware or software. Secrecy of the key and complexity of the cipher are crucial for the success of encryption controls.

- *Firewalls* - Firewalls are physical devices, software programs, or both, that enhance security by monitoring and limiting access to computer facilities. They create a security barrier between two or more networks to protect the institution's computer system from unauthorized entry. Filtering routers may be incorporated into the firewall system to screen data traffic and direct messages to certain locations.

Operations

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

- *Policies and Procedures* - Policies can be used to delineate management's expectations, benchmarks, and standard operating procedures. Standardized procedures will also help to provide consistent service.

- *Client Accounting* - Proper accounting for customer data will ensure that the institution's on-line PC banking activities involve pre-established accounts with authorized clients.

- *Contingency Plans* **-** Contingency plans can be used to minimize business disruptions caused by problems that impair or destroy the financial institution's processing and delivery systems. The plans should be tested periodically. Redundant systems should be considered as a means to provide back-up service.

- *Back up training* - Management should also provide backup training for key job functions so that human emergencies will not result in disrupted service.

- *Audit Procedures* - The system should be auditable and designed with attention to controls, including segregation of duties. Qualified internal and external auditors should evaluate the system's controls periodically.

PLANNING, TESTING, AND MONITORING

Financial institutions should evaluate the risks associated with PC banking and implement sound controls. Management and the Board should implement a comprehensive program to manage the inherent risks prior to implementation of PC banking activities. Representatives of all functional areas (e.g., audit, finance, information systems, legal, lending, and marketing) should be involved from the beginning of this process to collectively assess the potential effect on the overall institution. Existing controls should be expanded to address the risks of PC banking.

Planning, testing, and monitoring of PC banking activities should be conducted as part of the system development methodology and risk management process. PC banking involves an open and dynamic environment that requires continuous testing and monitoring. Threats to PC banking can come from both internal and external sources. Outside hackers, disgruntled employees, and inadvertent errors can adversely affect system reliability. Testing and monitoring of PC banking activities are integral parts of an institution's risk management process.

Although PC banking entails some risks requiring special consideration, standard operational controls common to computer environments still apply. Examples include contingency planning, information systems service contracts, and information security. The OTS Thrift Activities Regulatory Handbook, Section 341, Electronic Data Processing Controls offers additional guidance on evaluating electronic data processing risk.