Federal Financial Institutions Examination Council

2100 Pennsylvania Avenue, NW, Suite 200 . Washington, DC 20037
(202) 634-6526 . FAX (202) 634-6556

INTERAGENCY STATEMENT ON RETAIL ON-LINE PC BANKING

TO: Chief Executive Officers of all Federally Supervised Financial Institutions, Senior Management of each FFIEC Agency, and all Examining Personnel

I. PURPOSE

This statement alerts the Board of Directors and management to some of the risks and concerns of retail on-line, personal computer banking (PC banking). Recently, the staff of the FFIEC agencies organized a symposium to hear industry experts offer their thoughts and observations on the development of retail on-line PC banking. Through this statement, the FFIEC agencies wish to impart many of the ideas discussed during the symposium to bankers and examiners.

II. EXECUTIVE SUMMARY

Financial institutions are beginning to utilize new technologies to offer innovative products and services to their customers. On-line PC banking exemplifies an emerging delivery channel for retail banking services made possible by technology. One of the reasons for the rapid evolution of PC banking involves the increased use of the Internet[1]. Regulatory agencies recognize that PC banking offers opportunities for financial institutions to enhance customer relationships and improve competitive positions.

Before implementing a PC banking program, management should exercise sufficient due diligence and develop comprehensive plans. Such due diligence would ordinarily include the following activities.

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

[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.

An appendix is also provided which outlines a planning process for PC banking and a table which summarizes general risk categories and related controls.

III. BACKGROUND

Consumers of financial products and services are demanding greater convenience without sacrificing quality of service, confidentiality, and data integrity. Although financial institutions may face competitive pressures to rush to market with an on-line PC banking program, precautions must be taken to ensure data integrity, protect institution assets, and preserve customer confidence.

PC banking involves the use of a personal computer to interact with a financial institution. Customers can use their PC and modem to contact the bank via dial-up telephone lines connected directly to the institution, third-party vendors, or the Internet. 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 telephones, automated teller machines, televisions, and video kiosks. Although the devices and distribution channels are different. the risk and control issues delineated in this document are generally applicable, regardless of the access device.

Financial institutions will offer a wide range of services via the personal computer in the future. PC banking systems which deliver these services can be developed by financial institutions independently or in partnership with third-party providers. 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 bank products and services on the World Wide Web[2].

IV. RISKS AND CONTROLS

PC banking activities involve a wide range of potential risk exposures. Some of these risks are unique to this new delivery channel. while others represent general risks that are common to traditional banking practices. When implementing a PC banking program, management must ensure that unique risk 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.

General areas of risk 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

[2] The World Wide Web (WWW) 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".

general risk areas are explored more fully below, along with examples of compensating controls. Reference is made to Table I of the appendix which summarizes risk areas and related controls.

Strategic Risk

Strategic risk includes the business risks that a financial institution faces when new products or services are introduced. Specific concerns include the development of a positive business case which justifies the PC banking program. Sufficient resources must be provided to support the program and strategic decisions must be made regarding whether to outsource certain functions or perform them in-house.

Business Case

The decision to offer a PC banking program should be justified by a positive business case. Management must consider the resources required to implement the program, and the expected customer demand.

Strategic Technology Planning - Technology planning is a part of the strategic planning process. The financial institution should 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.

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

Internal and External Resources

Internal and external resources should be evaluated to determine their sufficiency relative to the demands of the PC banking program.

Provide Adequate Training - The institution's staff must be properly trained to implement the program. Specifically, they must 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) must be kept informed of any changes and/or updates to the program. Additional personnel may be needed to address an increased volume of customer inquiries.

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.

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/or embarrassment to a financial institution.

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.

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

Technological Developments

Technology is dynamic. In order to maintain a secure system that meets customer needs, financial institutions must remain abreast of technological developments. Systems should be upgraded as more sophisticated security techniques and user options are developed.

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 involves the uncertain legal framework in an electronic environment, jurisdiction issues, 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.

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.

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. Bank management should explore the use of digital signatures and monitor legal developments in this area.

Comprehensive Disclosures - Bank management must 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.

Consult with Legal Counsel - Prior to implementing a PC banking program, management should consult with legal counsel to identify and address relevant legal issues.

Well-defined Trade Area - Prior to implementing a PC banking program, management should 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.

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

Consult with Regulatory Agencies - Financial institutions should consult with their regulators as they consider and implement PC banking programs.

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

Operational Risk

Operational risk involves system security and reliability. 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

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 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. Parameters may be established such as dollar limits for transactions and restrictions on the number of transactions allowed.

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.

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

Authentication - Authentication is used to verify and recognize the identify 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.

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.

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.

V. PLANNING, TESTING, AND MONITORING

Financial institutions must 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 impact on the overall institution. Existing controls must 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 impact 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 *FFIEC Information Systems Examination Handbook* offers additional guidance on technological issues.

VI. CONCLUSION

Financial institutions are encouraged to use technological innovations to efficiently provide products and services to their customers. However, these innovations should not be employed without due consideration of the risks, controls, and costs. Refer to the attached appendix for additional details concerning the planning process for implementing a PC banking system and a table which summarizes general risk categories, areas of concern, and related controls.

The regulatory agencies want to remain knowledgeable of industry trends with respect to emerging technology. Financial institutions engaging in, or contemplating PC banking, or other remote banking activities, are encouraged to inform and consult with their primary federal regulator.

APPENDIX

PLANNING PROCESS FOR IMPLEMENTING PC BANKING

This appendix describes a process that management should consider in evaluating and implementing retail, on-line PC banking. Although this is one of several possible approaches to implementing new programs at financial institutions, it highlights certain key risks, issues, and concerns that management should address.

I. CONCEPTUALIZE AND PLAN

- **Develop a detailed plan**

  - State mission
  - Fit into overall corporate strategic plan
  - Consider alternative strategies
  - Establish means of performance measurement
  - Formulate success criteria
  - Determine deliverables and timetables
  - Gather information
  - Perform cost/benefit analysis that considers products, services, and distribution channels
  - Identify alternative courses of action in the event of project problems, delays. cancellations, or failure

- ***Assure Board of Directors' commitment, understanding, and awareness***

- ***Devote adequate resources***
  - Assure representation of relevant disciplines such as technical, legal, compliance, and audit
  - Assign human resources with adequate skills, knowledge, and expertise
  - Provide adequate funding and capital

- **Empower management group to proceed with the mission while keeping Board of Directors informed of progress**

II. IDENTIFY, ASSESS, AND MITIGATE

- ***Identify key risks***
  - Determine the types of risks and exposures within the context of the product, service, or distribution channel being considered.

- ***Assess the degree of risk exposure***
  - Qualify and quantify risks to the system
  - Recognize relative strengths and weaknesses of different controls

- ***Adopt and implement mitigating strategies***
  - Implement controls commensurate with the type and degree of risk
  - Balance the cost of risk reduction level with the value of the asset protected
  - Preserve safety and soundness and ensure compliance with consumer disclosure and protection requirements to maintain customer confidence and trust

III. CONSULT, DEVELOP, TEST, AND IMPLEMENT

Consult with Information Systems staff regarding Systems Development Life Cycle (SDLC) and System Development Methodology (SDM) for additional guidance.

- ***Gather expert opinions***
  - Communicate intentions with regulatory authority
  - Consult with legal counsel and insurers (bond provider)

- ***Develop or Purchase the System***

- ***Test***
  - To ensure the quality of the system, devise tests for determining the adequacy of controls, as well as operational and recovery ability

- ***Implement***
  - Ensure proper control over each implementation phase
  - Educate executives, employees, and customers to the level appropriate
  - Perform post implementation review

IV. MONITOR RESULTS AND MAINTAIN QUALITY CONTROL

- ***Review and assess***
  - Monitor transactions, exceptions, and overall performance
  - Conduct internal and external audits
  - Implement third party reviews and examinations
  - Conduct self assessments
  - Submit results to the Board of Directors and senior management for review

- ***Provide Customer Service***
  - Use market surveys and other techniques for customer analysis and feedback
  - Adopt problem and exception handling and resolution policies and procedures
  - Implement delivery standards and performance monitoring strategies

- ***Continue communications with all parties regarding latest developments***
- ***Provide adequate testing and timely distribution of software updates***

TABLE 1

General Risk Categories, Areas of Concern, and Related Controls

General Risk Category	Area of Concern	Related Control(s)
Strategic	Business Case	1. Strategic Technology Planning 2. Establish Goals and Monitor Performance 3. Conduct Research and Consult with Experts
	Internal/External Resources	1. Provide Adequate Training 2. Provide Adequate Support Staff 3. Administration of Software Updates 4. Insurance Coverage (e.g., Fidelity Bond)
	Outsourcing Arrangements	1. Perform Due Diligence on Vendors 2. Audit Performance 3. Back-up Arrangements
	Technological Developments	1. Monitor New Developments 2. Budget for Technology Upgrades
Legal/Regulatory	Legal Framework	1. Detailed Contracts 2. Digital Signature 3. Comprehensive Disclosures
	Jurisdiction (e.g., Laws, Taxes)	1. Consult with Legal Counsel 2. Well-defined Trade Area
	Regulatory Compliance	1. Policies and Procedures 2. Consult with Regulatory Agencies 3. Internal and External Audit

TABLE 1 (continued)

General Risk Category	Area of Concern	Related Control(s)
Operational	Security	1. Authorization 2. Access Control (e.g., Passwords, Log-on IS) 3. Authentication 4. Secure Data Storage 5. Encryption 6. Firewalls/Filtering Routers
	Operations	1. Policies and Procedures 2. Client Accounting 3. Contingency Plans 4. Back-up Training 5. Audit Procedures