Federal Financial Institutions Examination Council

FFIEC

E-Banking

EB

AUGUST 2003

IT Examination Handbook

Table of Contents

Introduction 1
Definition of E-Banking 1
Informational Websites 1
Transactional Websites 2
E-Banking Components 3
E-Banking Support Services 7
Weblinking 7
Account Aggregation 8
Electronic Authentication 8
Website Hosting 9
Payments for E-Commerce 10
Wireless E-Banking 13
E-Banking Risks 14
Transaction/Operations Risk 14
Credit Risk 14
Liquidity, Interest Rate, Price/Market Risks 15
Compliance/Legal Risk 15
Strategic Risk 17
Reputation Risk 17
Risk Management of E-Banking Activities 18
Board and Management Oversight 19
E-Banking Strategy 19
Cost-Benefit Analysis and Risk Assessment 20
Monitoring and Accountability 21
Audit 21
Managing Outsourcing Relationships 22
Due Diligence for Outsourcing Solutions 22

Contracts for Third-Party Services	24
Oversight and Monitoring of Third Parties	25
Information Security Program	26
Security Guidelines	27
Information Security Controls	28
Authenticating E-Banking Customers	30
Administrative controls	33
Internal Controls	34
Business Continuity Controls	35
Legal and Compliance Issues	36
Trade Names on the Internet	37
Website Content	37
Customer Privacy and Confidentiality	38
Transaction Monitoring and Consumer Disclosures	38
Appendix A: Examination Procedures	A-1
Appendix B: Glossary	B-1
Appendix C: Laws, Regulations, and Guidance	C-1
Appendix D: Aggregation Services	D-1
Appendix E: Wireless Banking	E-1

Introduction

This booklet, one of several comprising the FFIEC Information Technology Examination Handbook (IT Handbook), provides guidance to examiners and financial institutions on identifying and controlling the risks associated with electronic banking (e-banking) activities. The booklet primarily discusses e-banking risks from the perspective of the services or products provided to customers. This approach differs from other booklets that discuss risks from the perspective of the technology and systems that support automated information processing. To avoid duplication of material, this booklet refers the reader to other IT Handbook booklets for detailed explanations of technology-specific issues or controls.

Examiners may use the examination procedures and request letter items included in this booklet in appendix A to review risks in the electronic delivery of financial products and services. These procedures address services and products of varied complexity. Examiners should adjust the procedures, as appropriate, for the scope of the examination and the risk profile of the institution. The procedures may be used independently or in combination with procedures from other IT Handbook booklets or from agency handbooks covering non-IT areas.

Definition of E-Banking

For this booklet, e-banking is defined as the automated delivery of new and traditional banking products and services directly to customers through electronic, interactive communication channels. E-banking includes the systems that enable financial institution customers, individuals or businesses, to access accounts, transact business, or obtain information on financial products and services through a public or private network, including the Internet. Customers access e-banking services using an intelligent electronic device, such as a personal computer (PC), personal digital assistant (PDA), automated teller machine (ATM), kiosk, or Touch Tone telephone. While the risks and controls are similar for the various e-banking access channels, this booklet focuses specifically on Internet-based services due to the Internet's widely accessible public network. Accordingly, this booklet begins with a discussion of the two primary types of Internet websites: informational and transactional.

Informational Websites

Informational websites provide customers access to general information about the financial institution and its products or services. Risk issues examiners should consider when reviewing informational websites include:

- Potential liability and consumer violations for inaccurate or incomplete information about products, services, and pricing presented on the website;
- Potential access to confidential financial institution or customer information if the website is not properly isolated from the financial institution's internal network;

- Potential liability for spreading viruses and other malicious code to computers communicating with the institution's website; and
- Negative public perception if the institution's on-line services are disrupted or if its website is defaced or otherwise presents inappropriate or offensive material.

Transactional Websites

Transactional websites provide customers with the ability to conduct transactions through the financial institution's website by initiating banking transactions or buying products and services. Banking transactions can range from something as basic as a retail account balance inquiry to a large business-to-business funds transfer. E-banking services, like those delivered through other delivery channels, are typically classified based on the type of customer they support. The following table lists some of the common retail and wholesale e-banking services offered by financial institutions.

Table 1: Common E-Banking Services

Retail Services	Wholesale Services
Account management	Account management
Bill payment and presentment	Cash management
New account opening	Small business loan applications, approvals, or advances
Consumer wire transfers	
Investment/Brokerage services	Commercial wire transfers
Loan application and approval	Business-to-business payments
Account aggregation	Employee benefits/pension administration

Since transactional websites typically enable the electronic exchange of confidential customer information and the transfer of funds, services provided through these websites expose a financial institution to higher risk than basic informational websites. Wholesale e-banking systems typically expose financial institutions to the highest risk per transaction, since commercial transactions usually involve larger dollar amounts. In addition to the risk issues associated with informational websites, examiners reviewing transactional e-banking services should consider the following issues:

- Security controls for safeguarding customer information;
- Authentication processes necessary to initially verify the identity of new customers and authenticate existing customers who access e-banking services;
- Liability for unauthorized transactions;
- Losses from fraud if the institution fails to verify the identity of individuals or businesses applying for new accounts or credit on-line;
- Possible violations of laws or regulations pertaining to consumer privacy, anti-money laundering, anti-terrorism, or the content, timing, or delivery of required consumer disclosures; and
- Negative public perception, customer dissatisfaction, and potential liability resulting from failure to process third-party payments as directed or within specified time frames, lack of availability of on-line services, or unauthorized access to confidential customer information during transmission or storage.

E-Banking Components

E-banking systems can vary significantly in their configuration depending on a number of factors. Financial institutions should choose their e-banking system configuration, including outsourcing relationships, based on four factors:

- Strategic objectives for e-banking;
- Scope, scale, and complexity of equipment, systems, and activities;
- Technology expertise; and
- Security and internal control requirements.

Financial institutions may choose to support their e-banking services internally. Alternatively, financial institutions can outsource any aspect of their e-banking systems to third parties. The following entities could provide or host (i.e., allow applications to reside on their servers) e-banking-related services for financial institutions:

- Another financial institution,
- Internet service provider,
- Internet banking software vendor or processor,
- Core banking vendor or processor,
- Managed security service provider,

- Bill payment provider,
- Credit bureau, and
- Credit scoring company.

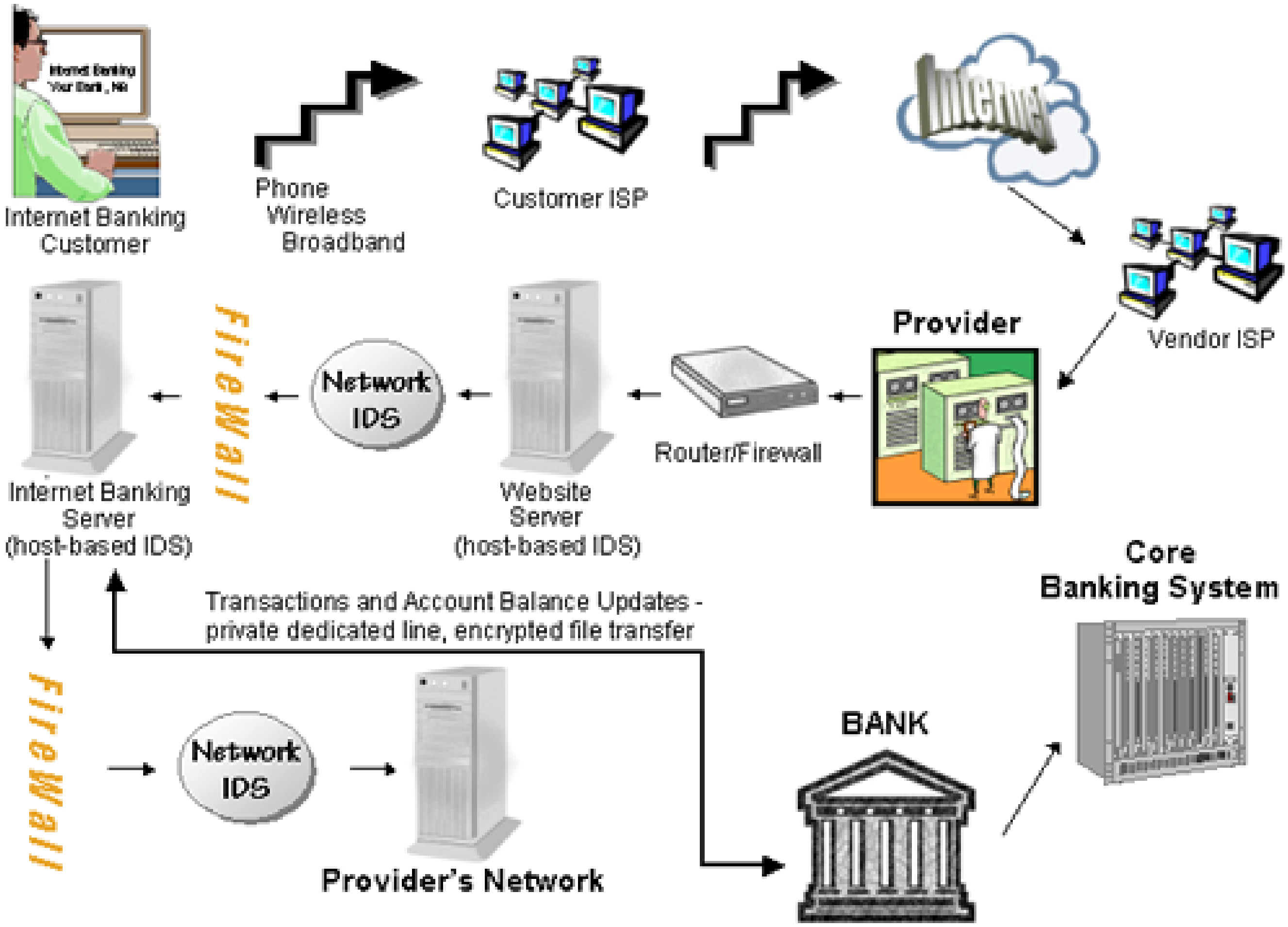
E-banking systems rely on a number of common components or processes. The following list includes many of the potential components and processes seen in a typical institution:

- Website design and hosting,
- Firewall configuration and management,
- Intrusion detection system or IDS (network and host-based),
- Network administration,
- Security management,
- Internet banking server,
- E-commerce applications (e.g., bill payment, lending, brokerage),
- Internal network servers,
- Core processing system,
- Programming support, and
- Automated decision support systems.

These components work together to deliver e-banking services. Each component represents a control point to consider.

Through a combination of internal and outsourced solutions, management has many alternatives when determining the overall system configuration for the various components of an e-banking system. However, for the sake of simplicity, this booklet presents only two basic variations. First, one or more technology service providers can host the e-banking application and numerous network components as illustrated in the following diagram. In this configuration, the institution's service provider hosts the institution's website, Internet banking server, firewall, and intrusion detection system. While the institution does not have to manage the daily administration of these component systems, its management and board remain responsible for the content, performance, and security of the e-banking system.

Figure 1: Third-Party Provider Hosted E-Banking Diagram


Internet Banking Your Bank, NA
Internet Banking Customer
Phone Wireless Broadband
Customer ISP
Internet
Vendor ISP
Provider
Router/Firewall
Website Server (host-based IDS)
Network IDS
FireWall
Internet Banking Server (host-based IDS)
Transactions and Account Balance Updates - private dedicated line, encrypted file transfer
Core Banking System
FireWall
Network IDS
Provider's Network
BANK

Text Description of Figure 1

This diagram illustrates the transaction flow for one possible configuration where the bank relies on a technology service provider to host its Internet banking application.

- Internet banking customer sends an e-banking transaction through their Internet Service Provider (ISP) via a phone, wireless, or broadband connection.

- The customer's ISP routes the transaction through the Internet and sends it to the e-banking service provider's ISP, which routes it to the provider.

- The transaction enters the provider's network through a router, which directs the e-banking transaction through a firewall to the application running on the Internet banking server.

- The website server and Internet banking server may have host-based intrusion detection system (IDS) software monitoring the server and its files to provide alerts of potential unauthorized modifications.

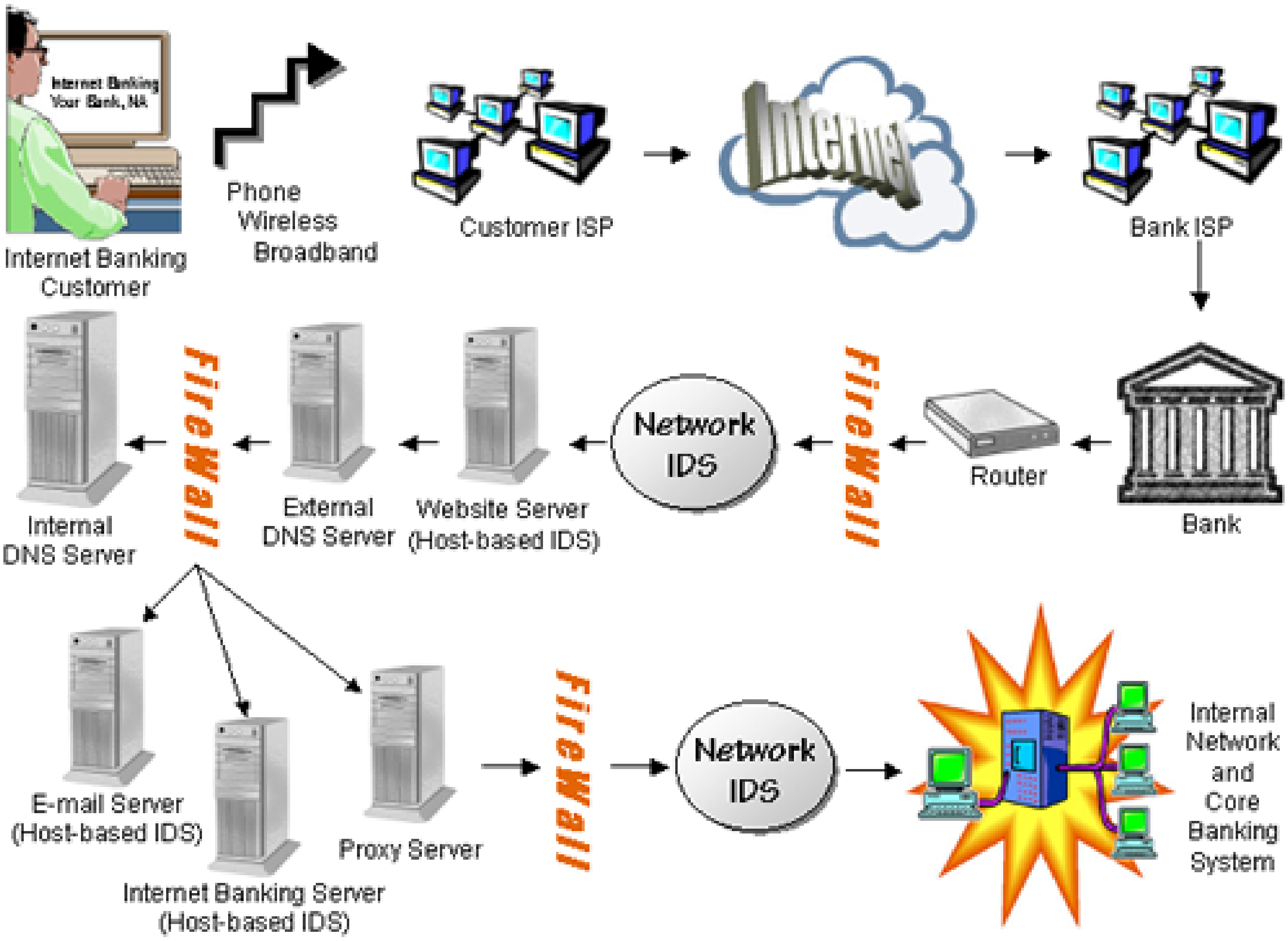
- Network IDS software may reside at different points within the network to analyze the message for potential attack characteristics that suggest an intrusion attempt.

- The Internet banking application processes the transaction against account balance data through a real time connection to the core banking system or a database of account balance data, which is updated periodically from the core banking system.

- The Internet banking server has a firewall filtering Internet traffic from its internal network.

Second, the institution can host all or a large portion of its e-banking systems internally. A typical configuration for in-house hosted, e-banking services is illustrated below. In this case, a provider is not between the Internet access and the financial institution's core processing system. Thus, the institution has day-to-day responsibility for system administration.

Figure 2: In-House E-Banking Diagram



Text Description of Figure 2 This diagram illustrates the transaction flow for one possible configuration in which the bank hosts the Internet banking application.

- Internet banking customer sends an e-banking transaction through their Internet Service Provider (ISP) via a phone, wireless, or broadband connection.

- The customer's ISP routes the transaction through the Internet and sends it to the e-banking service bank's ISP, which routes it the provider.

- The transaction enters the bank's network through a router, which directs the Internet-banking transaction through a firewall to the application running on the Internet banking server.

- The bank typically has several Internet application servers that could include a website server, e-mail server, proxy server, and domain name server (DNS) in addition to the Internet banking application server.

- The router will typically send the transaction around the other application servers directly to the Internet banking server unless it is a non-banking transaction.

- The website server and Internet banking server may have host-based intrusion detection system (IDS) software monitoring the server and its files to provide alerts of potential unauthorized modifications.

- Network IDS software may reside at different points within the network to analyze the message for potential attack characteristics that suggest an unauthorized intrusion attempt.

- The Internet banking application processes the transaction against account balance data through a real time connection to the core banking system or a database of account balance data, which is updated periodically from the core banking system.

- The Internet banking server has a firewall filtering Internet traffic from the bank's internal network.

E-Banking Support Services

In addition to traditional banking products and services, financial institutions can provide a variety of services that have been designed or adapted to support e-commerce. Management should understand these services and the risks they pose to the institution. This section discusses some of the most common support services: weblinking, account aggregation, electronic authentication, website hosting, payments for e-commerce, and wireless banking activities.

Weblinking

A large number of financial institutions maintain sites on the World Wide Web. Some websites are strictly informational, while others also offer customers the ability to perform financial transactions, such as paying bills or transferring funds between accounts.

Virtually every website contains "weblinks." A weblink is a word, phrase, or image on a webpage that contains coding that will transport the viewer to a different part of the website or a completely different website by just clicking the mouse. While weblinks are a convenient and accepted tool in website design, their use can present certain risks.

Generally, the primary risk posed by weblinking is that viewers can become confused about whose website they are viewing and who is responsible for the information, products, and services available through that website. There are a variety of risk management techniques institutions should consider using to mitigate these risks. These risk management techniques are for those institutions that develop and maintain their own websites, as well as institutions that use third-party service providers for this function. The agencies have issued guidance on weblinking that provides details on risks and risk management techniques financial institutions should consider.See the interagency guidance titled "Weblinking: Identifying Risks and Risk Management Techniques" issued April 23, 2003 by the Federal Deposit Insurance Corporation (FDIC), National Credit Union Administration (NCUA), Office of the Comptroller of the Currency (OCC), and Office of Thrift Supervision (OTS) (the agencies) for specific risk and risk management guidance.

Account Aggregation

Account aggregation is a service that gathers information from many websites, presents that information to the customer in a consolidated format, and, in some cases, may allow the customer to initiate activity on the aggregated accounts. The information gathered or aggregated can range from publicly available information to personal account information (e.g., credit card, brokerage, and banking data). Aggregation services can improve customer convenience by avoiding multiple log-ins and providing access to tools that help customers analyze and manage their various account portfolios. Some aggregators use the customer-provided user IDs and passwords to sign in as the customer. Once the customer's account is accessed, the aggregator copies the personal account information from the website for representation on the aggregator's site (i.e., "screen scraping"). Other aggregators use direct data-feed arrangements with website operators or other firms to obtain the customer's information. Generally, direct data feeds are thought to provide greater legal protection to the aggregator than does screen scraping.

Financial institutions are involved in account aggregation both as aggregators and as aggregation targets. Risk management issues examiners should consider when reviewing aggregation services include:

- Protection of customer passwords and user IDs - both those used to access the institution's aggregation services and those the aggregator uses to retrieve customer information from aggregated third parties - to assure the confidentiality of customer information and to prevent unauthorized activity,
- Disclosure of potential customer liability if customers share their authentication information (i.e., IDs and passwords) with third parties, and
- Assurance of the accuracy and completeness of information retrieved from the aggregated parties' sites, including required disclosures

Additional information regarding management of risks in aggregation services can be found in appendix D.

Electronic Authentication

Verifying the identities of customers and authorizing e-banking activities are integral parts of e-banking financial services. Since traditional paper-based and in-person identity authentication methods reduce the speed and efficiency of electronic transactions, financial institutions have adopted alternative authentication methods, including:

- Passwords and personal identification numbers (PINs),
- Digital certificates using a public key infrastructure (PKI),
- Microchip-based devices such as smart cards or other types of tokens,
- Database comparisons (e.g., fraud-screening applications), and
- Biometric identifiers.

The authentication methods listed above vary in the level of security and reliability they provide and in the cost and complexity of their underlying infrastructures. As such, the choice of which technique(s) to use should be commensurate with the risks in the products and services for which they control access.For example, section 326 of the USA PATRIOT Act (Pub. L. 107-56) requires financial institutions to implement reasonable procedures for (1) verifying the identity of any person seeking to open an account, to the extent reasonable and practicable; (2) maintaining records of the information used to verify the person's identity, and (3) determining whether the person appears on any list of known or suspected terrorists or terrorist organizations. See 68 Federal Register 25090 (May 9, 2003); 12 CFR Part 21 (OCC); 12 CFR Parts 208 and 211 (Board); 12 CFR Part 326 (FDIC); 12 CFR Part 563 (OTS), and 12 CFR Part 748 (NCUA). Additional information on customer authentication techniques can be found in this booklet under the heading "Authenticating E-Banking Customers."

The Electronic Signatures in Global and National Commerce (E-Sign) Act establishes some uniform federal rules concerning the legal status of electronic signatures and records in commercial and consumer transactions so as to provide more legal certainty and promote the growth of electronic commerce.Pub.L. No. 106-229. An electronic signature may be as simple as a person's typed name or an image of a person's handwritten signature. The development of secure digital signatures continues to evolve with some financial institutions either acting as the certification authority for digital signatures or providing repository services for digital certificates.See OCC Bulletin 99-20: Certificate Authority Guidance (May 4, 1999).

Website Hosting

Some financial institutions host websites for both themselves as well as for other businesses. Financial institutions that host a business customer's website usually store, or arrange for the storage of, the electronic files that make up the website. These files are stored on one or more servers that may be located on the hosting financial institution's premises. Website hosting services require strong skills in networking, security, and programming. The technology and software change rapidly. Institutions developing websites should monitor the need to adopt new interoperability standards and protocols such as Extensible Mark-Up Language (XML) to facilitate data exchange among the diverse population of Internet users.

Risk issues examiners should consider when reviewing website hosting services include damage to reputation, loss of customers, or potential liability resulting from:

- Downtime (i.e., times when website is not available) or inability to meet service levels specified in the contract,
- Inaccurate website content (e.g., products, pricing) resulting from actions of the institution's staff or unauthorized changes by third parties (e.g., hackers),
- Unauthorized disclosure of confidential information stemming from security breaches, and
- Damage to computer systems of website visitors due to malicious code (e.g., virus, worm, active content) spread through institution-hosted sites.

Payments for E-Commerce

Many businesses accept various forms of electronic payments for their products and services. Financial institutions play an important role in electronic payment systems by creating and distributing a variety of electronic payment instruments, accepting a similar variety of instruments, processing those payments, and participating in clearing and settlement systems. However, increasingly, financial institutions are competing with third parties to provide support services for e-commerce payment systems. Among the electronic payments mechanisms that financial institutions provide for e-commerce are automated clearing house (ACH) debits and credits through the Internet, electronic bill payment and presentment, electronic checks, e-mail money, and electronic credit card payments. Additional information on payments systems can be found in other sections of the IT Handbook.

Most financial institutions permit intrabank transfers between a customer's accounts as part of their basic transactional e-banking services. However, third-party transfers - with their heightened risk for fraud - often require additional security safeguards in the form of additional authentication and payment confirmation.

Bill Payment and Presentment

Bill payment services permit customers to electronically instruct their financial institution to transfer funds to a business's account at some future specified date. Customers can make payments on a one-time or recurring basis, with fees typically assessed as a "per item" or monthly charge. In response to the customer's electronic payment instructions, the financial institution (or its bill payment provider) generates an electronic transaction - usually an automated clearinghouse (ACH) credit - or mails a paper check to the business on the customer's behalf. To allow for the possibility of a paper-based transfer, financial institutions typically advise customers to make payments effective 3-7 days before the bill's due date.

Internet-based cash management is the commercial version of retail bill payment. Business customers use the system to initiate third-party payments or to transfer money between company accounts. Cash management services also include minimum balance maintenance, recurring transfers between accounts and on-line account reconciliation. Businesses typically require stronger controls, including the ability to administer security and transaction controls among several users within the business.

This booklet discusses the front-end controls related to the initiation, storage, and transmission of bill payment transactions prior to their entry into the industry's retail payment systems (e.g., ACH, check processing, etc.). The IT Handbook's "Retail Payments Systems Booklet" provides additional information regarding the various electronic transactions that comprise the back end for bill payment processing. The extent of front-end operating controls directly under the financial institution's control varies with the system configuration. Some examples of typical configurations are listed below in order of increasing complexity, along with potential control considerations.

- Financial institutions that do not provide bill payment services, but may direct customers to select from several unaffiliated bill payment providers.

  - Caution customers regarding security and privacy issues through the use of on-line disclosures or, more conservatively, e-banking agreements.

- Financial institutions that rely on a third-party bill payment provider including Internet banking providers that subcontract to third parties.

  - Set dollar and volume thresholds and review bill payment transactions for suspicious activity.

  - Gain independent audit assurance over the bill payment provider's processing controls.

  - Restrict employees' administrative access to ensure that the internal controls limiting their capabilities to originate, modify, or delete bill payment transactions are at least as strong as those applicable to the underlying retail payment system ultimately transmitting the transaction.

  - Restrict by vendor contract and identify the use of any subcontractors associated with the bill payment application to ensure adequate oversight of underlying bill payment system performance and availability.

  - Evaluate the adequacy of authentication methods given the higher risk associated with funds transfer capabilities rather than with basic account access.

  - Consider the additional guidance contained in the IT Handbook's "Information Security," "Retail Payment Systems," and "Outsourcing Technology Services" booklets.

- Financial institutions that use third-party software to host a bill payment application internally.

  - Determine the extent of any independent assessments or certification of the security of application source code.

- Ensure software is adequately tested prior to installation on the live system.

- Ensure vendor access for software maintenance is controlled and monitored.

- Financial institutions that develop, maintain, and host their own bill payment system.

  - Consider additional guidance in the IT Handbook's "Development and Acquisition Booklet."

Financial institutions can offer bill payment as a stand-alone service or in combination with bill presentment. Bill presentment arrangements permit a business to submit a customer's bill in electronic form to the customer's financial institution. Customers can view their bills by clicking on links on their account's e-banking screen or menu. After viewing a bill, the customer can initiate bill payment instructions or elect to pay the bill through a different payment channel.

In addition, some businesses have begun offering electronic bill presentment directly from their own websites rather than through links on the e-banking screens of a financial institution. Under such arrangements, customers can log on to the business's website to view their periodic bills. Then, if so desired, they can electronically authorize the business to "take" the payment from their account. The payment then occurs as an ACH debit originated by the business's financial institution as compared to the ACH credit originated by the customer's financial institution in the bill payment scenario described above. Institutions should ensure proper approval of businesses allowed to use ACH payment technology to initiate payments from customer accounts.

Cash management applications would include the same control considerations described above, but the institution should consider additional controls because of the higher risk associated with commercial transactions. The adequacy of authentication methods becomes a higher priority and requires greater assurance due to the larger average dollar size of transactions. Institutions should also establish additional controls to ensure binding agreements - consistent with any existing ACH or wire transfer agreements - exist with commercial customers. Additionally, cash management systems should provide adequate security administration capabilities to enable the business owners to restrict access rights and dollar limits associated with multiple-user access to their accounts.

Person-to-Person Payments

Electronic person-to-person payments, also known as e-mail money, permit consumers to send "money" to any person or business with an e-mail address. Under this scenario, a consumer electronically instructs the person-to-person payment service to transfer funds to another individual. The payment service then sends an e-mail notifying the individual that the funds are available and informs him or her of the methods available to access the funds including requesting a check, transferring the funds to an account at an insured financial institution, or retransmitting the funds to someone else. Person-to-person payments are typically funded by credit card charges or by an ACH transfer from the consumer's account at a financial institution. Since neither the payee nor the payer in the transaction has to have an account with the payment service, such services may be offered by an insured financial institution, but are frequently offered by other businesses as well.

Some of the risk issues examiners should consider when reviewing bill payment, presentment, and e-mail money services include:

- Potential liability for late payments due to service disruptions,
- Liability for bill payment instructions originating from someone other than the deposit account holder,
- Losses from person-to-person payments funded by transfers from credit cards or deposit accounts over which the payee does not have signature authority,
- Losses from employee misappropriation of funds held pending access instructions from the payer, and
- Potential liability directing payment availability information to the wrong e-mail or for releasing funds in response to e-mail from someone other than the intended payee.

Wireless E-Banking

Wireless banking is a delivery channel that can extend the reach and enhance the convenience of Internet banking products and services. Wireless banking occurs when customers access a financial institution's network(s) using cellular phones, pagers, and personal digital assistants (or similar devices) through telecommunication companies' wireless networks. Wireless banking services in the United States typically supplement a financial institution's e-banking products and services.

Wireless devices have limitations that increase the security risks of wireless-based transactions and that may adversely affect customer acceptance rates. Device limitations include reduced processing speeds, limited battery life, smaller screen sizes, different data entry formats, and limited capabilities to transfer stored records. These limitations combine to make the most recognized Internet language, Hypertext Markup Language (HTML), ineffective for delivering content to wireless devices. Wireless Markup Language (WML) has emerged as one of a few common language standards for developing wireless device content. Wireless Application Protocol (WAP) has emerged as a data transmission standard to deliver WML content.

Manufacturers of wireless devices are working to improve device usability and to take advantage of enhanced "third-generation" (3G) services. Device improvements are anticipated to include bigger screens, color displays, voice recognition applications, location identification technology (e.g., Federal Communications Commission (FCC) Enhanced 911), and increased battery capacity. These improvements are geared towards increasing customer acceptance and usage. Increased communication speeds and improvements in devices during the next few years should lead to continued increases in wireless subscriptions.

As institutions begin to offer wireless banking services to customers, they should consider the risks and necessary risk management controls to address security, authentication, and compliance issues. Some of the unique risk factors associated with wireless banking that may increase a financial institution's strategic, transaction, reputation, and compliance risks are discussed in appendix E.

E-Banking Risks

The practice of holding a check at the institution at which it was deposited (or at an intermediary institution) and electronically forwarding the essential information on the check to the institution on which it was written. A truncated check is not returned to the writer.

Transaction/Operations Risk

Transaction/Operations risk arises from fraud, processing errors, system disruptions, or other unanticipated events resulting in the institution's inability to deliver products or services. This risk exists in each product and service offered. The level of transaction risk is affected by the structure of the institution's processing environment, including the types of services offered and the complexity of the processes and supporting technology.

In most instances, e-banking activities will increase the complexity of the institution's activities and the quantity of its transaction/operations risk, especially if the institution is offering innovative services that have not been standardized. Since customers expect e-banking services to be available 24 hours a day, 7 days a week, financial institutions should ensure their e-banking infrastructures contain sufficient capacity and redundancy to ensure reliable service availability. Even institutions that do not consider e-banking a critical financial service due to the availability of alternate processing channels, should carefully consider customer expectations and the potential impact of service disruptions on customer satisfaction and loyalty.

The key to controlling transaction risk lies in adapting effective polices, procedures, and controls to meet the new risk exposures introduced by e-banking. Basic internal controls including segregation of duties, dual controls, and reconcilements remain important. Information security controls, in particular, become more significant requiring additional processes, tools, expertise, and testing. Institutions should determine the appropriate level of security controls based on their assessment of the sensitivity of the information to the customer and to the institution and on the institution's established risk tolerance level. Security controls are discussed in this booklet's "Risk Management of E-Banking Activities" section under the heading "Information Security Program."

Credit Risk

Generally, a financial institution's credit risk is not increased by the mere fact that a loan is originated through an e-banking channel. However, management should consider additional precautions when originating and approving loans electronically, including assuring management information systems effectively track the performance of portfolios originated through e-banking channels. The following aspects of on-line loan origination and approval tend to make risk management of the lending process more challenging. If not properly managed, these aspects can significantly increase credit risk.

- Verifying the customer's identity for on-line credit applications and executing an enforceable contract;
- Monitoring and controlling the growth, pricing, underwriting standards, and ongoing credit quality of loans originated through e-banking channels;
- Monitoring and oversight of third-parties doing business as agents or on behalf of the financial institution (for example, an Internet loan origination site or electronic payments processor);
- Valuing collateral and perfecting liens over a potentially wider geographic area;
- Collecting loans from individuals over a potentially wider geographic area; and
- Monitoring any increased volume of, and possible concentration in, out-of-area lending.

Liquidity, Interest Rate, Price/Market Risks

Funding and investment-related risks could increase with an institution's e-banking initiatives depending on the volatility and pricing of the acquired deposits. The Internet provides institutions with the ability to market their products and services globally. Internet-based advertising programs can effectively match yield-focused investors with potentially high-yielding deposits. But Internet-originated deposits have the potential to attract customers who focus exclusively on rates and may provide a funding source with risk characteristics similar to brokered deposits. An institution can control this potential volatility and expanded geographic reach through its deposit contract and account opening practices, which might involve face-to-face meetings or the exchange of paper correspondence. The institution should modify its policies as necessary to address the following e-banking funding issues:

- Potential increase in dependence on brokered funds or other highly rate-sensitive deposits;See "Joint Agency Advisory on Brokered and Rate-Sensitive Deposits," issued May 11, 2001.
- Potential acquisition of funds from markets where the institution is not licensed to engage in banking, particularly if the institution does not establish, disclose, and enforce geographic restrictions;
- Potential impact of loan or deposit growth from an expanded Internet market, including the impact of such growth on capital ratios; and
- Potential increase in volatility of funds should e-banking security problems negatively impact customer confidence or the market's perception of the institution.

Compliance/Legal Risk

Compliance and legal issues arise out of the rapid growth in usage of e-banking and the differences between electronic and paper-based processes. E-banking is a new delivery channel where the laws and rules governing the electronic delivery of certain financial institution products or services may be ambiguous or still evolving. Specific regulatory and legal challenges include:

- Uncertainty over legal jurisdictions and which state's or country's laws govern a specific e-banking transaction,
- Delivery of credit and deposit-related disclosures/notices as required by law or regulation,
- Retention of required compliance documentation for on-line advertising, applications, statements, disclosures and notices; and
- Establishment of legally binding electronic agreements.

Laws and regulations governing consumer transactions require specific types of disclosures, notices, or record keeping requirements. These requirements also apply to e-banking, and federal banking agencies continue to update consumer laws and regulations to reflect the impact of e-banking and on-line customer relationships. Some of the legal requirements and regulatory guidance that frequently apply to e-banking products and services include:

- Solicitation, collection and reporting of government monitoring information on applications and loans, as required by Equal Credit Opportunity Act (Regulation B) and Home Mortgage Disclosure Act (Regulation C) regulations;
- Advertising requirements, customer disclosures, or notices required by the Real Estate Settlement Procedures Act (RESPA), Truth in Lending (Regulation Z), and Truth In Savings (Regulation DD) and Fair Housing regulations;
- Proper and conspicuous display of FDIC or NCUA insurance notices;
- Conspicuous webpage disclosures indicating that certain types of investment, brokerage, and insurance products offered have certain associated risks, including not being insured by federal deposit insurance (FDIC or NCUA);
- Customer identification programs and procedures, as well as record retention and customer notification requirements, required by the Bank Secrecy Act;
- Customer identification processes to determine whether transactions are prohibited by the Office of Foreign Asset Control (OFAC) and, when necessary, whether customers appear on any list of known or suspected terrorists or terrorist organization provided by any government agency;
- Delivery of privacy and opt-out notices by hand, by mail, or with customer acknowledgement of electronic receipt;Required by regulations required by the Gramm-Leach-Bliley Act. See 12 CFR 40.9 (OCC), 12 CFR 216.9 (Board), 12 CFR 332.9 (FDIC), 12 CFR 573.9 (OTS), and 12 CFR 716.9 (NCUA).

- Verification of customer identification, reporting, and record keeping requirements of the Bank Secrecy Act (BSA), including requirements for filing a suspicious activity report (SAR); and
- Record retention requirements of the Equal Credit Opportunity Act (Regulation B) and Fair Credit Reporting Act regulations.

Institutions that offer e-banking services, both informational and transactional, assume a higher level of compliance risk because of the changing nature of the technology, the speed at which errors can be replicated, and the frequency of regulatory changes to address e-banking issues. The potential for violations is further heightened by the need to ensure consistency between paper and electronic advertisements, disclosures, and notices. Additional information on compliance requirements for e-banking can be found on the agencies' websites and in references contained in appendix C.

Strategic Risk

A financial institution's board and management should understand the risks associated with e-banking services and evaluate the resulting risk management costs against the potential return on investment prior to offering e-banking services. Poor e-banking planning and investment decisions can increase a financial institution's strategic risk. Early adopters of new e-banking services can establish themselves as innovators who anticipate the needs of their customers, but may do so by incurring higher costs and increased complexity in their operations. Conversely, late adopters may be able to avoid the higher expense and added complexity, but do so at the risk of not meeting customer demand for additional products and services. In managing the strategic risk associated with e-banking services, financial institutions should develop clearly defined e-banking objectives by which the institution can evaluate the success of its e-banking strategy. In particular, financial institutions should pay attention to the following:

- Adequacy of management information systems (MIS) to track e-banking usage and profitability;
- Costs involved in monitoring e-banking activities or costs involved in overseeing e-banking vendors and technology service providers;
- Design, delivery, and pricing of services adequate to generate sufficient customer demand;
- Retention of electronic loan agreements and other electronic contracts in a format that will be admissible and enforceable in litigation;
- Costs and availability of staff to provide technical support for interchanges involving multiple operating systems, web browsers, and communication devices;
- Competition from other e-banking providers; and
- Adequacy of technical, operational, compliance, or marketing support for e-banking products and services.

Reputation Risk

An institution's decision to offer e-banking services, especially the more complex transactional services, significantly increases its level of reputation risk. Some of the ways in which e-banking can influence an institution's reputation include:

- Loss of trust due to unauthorized activity on customer accounts,
- Disclosure or theft of confidential customer information to unauthorized parties (e.g., hackers),
- Failure to deliver on marketing claims,
- Failure to provide reliable service due to the frequency or duration of service disruptions,
- Customer complaints about the difficulty in using e-banking services and the inability of the institution's help desk to resolve problems, and
- Confusion between services provided by the financial institution and services provided by other businesses linked from the website.

Risk Management of E-Banking Activities

As noted in the prior section, e-banking has unique characteristics that may increase an institution's overall risk profile and the level of risks associated with traditional financial services, particularly strategic, operational, legal, and reputation risks. These unique e-banking characteristics include:

- Speed of technological change,
- Changing customer expectations,
- Increased visibility of publicly accessible networks (e.g., the Internet),
- Less face-to-face interaction with financial institution customers,
- Need to integrate e-banking with the institution's legacy computer systems,
- Dependence on third parties for necessary technical expertise, and
- Proliferation of threats and vulnerabilities in publicly accessible networks.

Management should review each of the processes discussed in this section to adapt and expand the institution's risk management practices as necessary to address the risks posed by e-banking activities. While these processes mirror those discussed in other booklets of the IT Handbook, they are discussed below from an e-banking perspective. For more detailed information on each of these processes, the reader should review the corresponding booklet of the IT Handbook.

Board and Management Oversight

Action Summary

The board of directors and senior management are responsible for developing the institution's e-banking business strategy, which should include:

- The rationale and strategy for offering e-banking services including informational, transactional, or e-commerce support;
- A cost-benefit analysis, risk assessment, and due diligence process for evaluating e-banking processing alternatives including third-party providers;
- Goals and expectations that management can use to measure the e-banking strategy's effectiveness; and
- Accountability for the development and maintenance of risk management policies and controls to manage e-banking risks and for the audit of e-banking activities

E-Banking Strategy

Financial institution management should choose the level of e-banking services provided to various customer segments based on customer needs and the institution's risk assessment considerations. Institutions should reach this decision through a board-approved, e-banking strategy that considers factors such as customer demand, competition, expertise, implementation expense, maintenance costs, and capital support. Some institutions may choose not to provide e-banking services or to limit e-banking services to an informational website. Financial institutions should periodically re-evaluate this decision to ensure it remains appropriate for the institution's overall business strategy. Institutions may define success in many ways including growth in market share, expanding customer relationships, expense reduction, or new revenue generation. If the financial institution determines that a transactional website is appropriate, the next decision is the range of products and services to make available electronically to its customers.OTS-regulated institutions must send a notice in conformance with 12 CFR 555, "Electronic Operations" prior to establishing a transactional website. To deliver those products and services, the financial institution may have more than one website or multiple pages within a website for various business lines.

Cost-Benefit Analysis and Risk Assessment

Financial institutions should base any decision to implement e-banking products and services on a thorough analysis of the costs and benefits associated with such action. Some of the reasons institutions offer e-banking services include:

- Lower operating costs,
- Greater geographic diversification,
- Improved or sustained competitive position,
- Increased customer demand for services, and
- New revenue opportunities.

The individuals conducting the cost-benefit analysis should clearly understand the risks associated with e-banking so that cost considerations fully incorporate appropriate risk mitigation controls. Without such expertise, the cost-benefit analysis will most likely underestimate the time and resources needed to properly oversee e-banking activities, particularly the level of technical expertise needed to provide competent oversight of in-house or outsourced activities. In addition to the obvious costs for personnel, hardware, software, and communications, the analysis should also consider:

- Changes to the institution's policies, procedures, and practices;
- The impact on processing controls for legacy systems;
- The appropriate networking architecture, security expertise, and software
- tools to maintain system availability and to protect and respond to unauthorized access attempts;
- The skilled staff necessary to support and market e-banking services during expanded hours and over a wider geographic area, including possible expanded market and cross-border activity;
- The additional expertise and MIS needed to oversee e-banking vendors or technology service providers;
- The higher level of legal, compliance, and audit expertise needed to support technology-dependent services;
- Expanded MIS to monitor e-banking security, usage, and profitability and to measure the success of the institution's e-banking strategy;
- Cost of insurance coverage for e-banking activities;

- Potential revenues under different pricing scenarios;
- Potential losses due to fraud; and
- Opportunity costs associated with allocating capital to e-banking efforts.

Monitoring and Accountability

Once an institution implements its e-banking strategy, the board and management should periodically evaluate the strategy's effectiveness. A key aspect of such an evaluation is the comparison of actual e-banking acceptance and performance to the institution's goals and expectations. Some items that the institution might use to monitor the success and cost effectiveness of its e-banking strategy include:

- Revenue generated,
- Website availability percentages,
- Customer service volumes,
- Number of customers actively using e-banking services,
- Percentage of accounts signed up for e-banking services, and
- The number and cost per item of bill payments generated.

Without clearly defined and measurable goals, management will be unable to determine if e-banking services are meeting the customers' needs as well as the institution's growth and profitability expectations.

In evaluating the effectiveness of the institution's e-banking strategy, the board should also consider whether appropriate policies and procedures are in effect and whether risks are properly controlled. Unless the initial strategy establishes clear accountability for the development of policies and controls, the board will be unable to determine where and why breakdowns in the risk control process occurred.

Audit

An important component of monitoring is an appropriate independent audit function. Financial institutions offering e-banking products and services should expand their audit coverage commensurate with the increased complexity and risks inherent in e-banking activities. Financial institutions offering e-banking services should ensure the audit program expands to include:

- Scope and coverage, including the entire e-banking process as applicable (i.e., network configuration and security, interfaces to legacy systems, regulatory compliance, internal controls, and support activities performed by third-party providers);

- Personnel with sufficient technical expertise to evaluate security threats and controls in an open network (i.e., the Internet); and
- Independent individuals or companies conducting the audits without conflicting e-banking or network security roles.

Managing Outsourcing Relationships

Action Summary

The board and senior management must provide effective oversight of third-party vendors providing e-banking services and support. Effective oversight requires that institutions ensure the following practices are in place:

- Effective due diligence in the selection of new service providers that considers financial condition, experience, expertise, technological compatibility, and customer satisfaction;
- Written contracts with specific provisions protecting the privacy and security of an institution's data, the institution's ownership of the data, the right to audit security and controls, and the ability to monitor the quality of service, limit the institution's potential liability for acts of the service provider, and terminate the contract;
- Appropriate processes to monitor vendor's ongoing performance, service quality, security controls, financial condition, and contract compliance; and
- Monitoring reports and expectations including incidence response and notification.

Due Diligence for Outsourcing Solutions

A key consideration in preparing an e-banking cost-benefit analysis is whether the financial institution supports e-banking services in-house or outsources support to one or more third parties (i.e., a technology service provider or TSP). Transactional e-banking is typically a front-end system that relies on a programming link called an interface to transfer information and transactions between the e-banking system and the institution's core processing applications (e.g., loans, deposits, asset management). Such interfaces can be between in-house systems, outsourced systems, or a combination of both. This flexibility allows institutions to select those products and services that best meet their e-banking needs, but it can also complicate the vendor oversight process when multiple vendors are involved. Choosing to use the services of one or more TSPs can help financial institutions manage costs, obtain necessary expertise, expand customer product offerings, and improve service quality. However, this choice does not absolve financial institutions from understanding and managing the risks associated with TSP services. In fact, service providers may introduce additional risks and interdependencies that financial institutions must understand and manage.

Table 2 below summarizes some of the advantages and disadvantages of supporting technology-based products and services in-house versus contracting for support with a TSP. Regardless of whether an institution's e-banking services are outsourced or processed in-house, the institution should periodically review whether this arrangement continues to meet current and anticipated future needs.

Table 2: Advantages and Disadvantages of Common Processing Alternatives

Processing Hardware	Application Software	Advantages	Disadvantages
In-house Purchased or Leased	Developed in-house	Systems designed to meet institution's specific needs. Ability to offer unique products and services. Direct oversight of risks.	Costs to develop/ maintain system. Requires high level of technical expertise.
Purchased with in-house modifications	Cheaper than in-house developed, while retaining ability to adapt system and directly oversee risks.	Cost of technical expertise to maintain system, modify vendor's software, and integrate vendor updates.	
Purchased without modifications	Requires lower level of expertise to maintain system and applications. Direct oversight of risks.	Limited ability to customize products/services and differentiate unique products.	

Outsourced To TSP	Outsourced To TSP	Minimal need for technical expertise.	No ownership interest.
		Increases implementation speed.	Limited ability to customize products/services.
		Lower start-up costs.	Need processes to oversee risks in outsourced activities or services.

Contracts for Third-Party Services

As with all outsourced financial services, institutions must have a formal contract with the TSP that clearly addresses the duties and responsibilities of the parties involved. In the past, some institutions have had informal security expectations for software vendors or Internet access providers that had never been committed to writing. This lack of clear responsibilities and consensus has lead to breakdowns in internal controls and allowed security incidents to occur. The IT Handbook's "Outsourcing Technology Services Booklet" lists detailed contract recommendations for TSPs. Institutions should tailor these recommendations to e-banking services as necessary. Specific examples of e-banking contract issues include:

- Restrictions on use of nonpublic customer information collected or stored by the TSP;Required in each of the Agencies' privacy regulations. The regulations are comparable to and consistent with one another. See 65 Federal Register 35,162 (June 1, 2000) (Board, FDIC, OCC, OTS); 65 Fed. Reg. 31740 (May 18, 2000) (NCUA); 12 CFR Parts 40 (OCC), 216 (Board), 332 (FDIC), and 573 (OTS), and 716 (NCUA).
- Requirements for appropriate controls to protect the security of customer information held by the TSP;Described in the "Interagency Guidelines Establishing Standards for Safeguarding Customer Information" (guidelines). See 66 Federal Register 8616 (Feb. 1, 2001); 12 CFR Part 30, app. B (OCC); 12 CFR Part 208, app. D-2 and Part 225, app. F (Board); 12 CFR Part 364, app. B (FDIC); 12 CFR Part 570, app. B (OTS).
- Service-level standards such as website "up-time," hyperlink performance, customer service response times, etc.;
- Incident response plans, including notification responsibilities, to respond to website outage, defacement, unauthorized access, or malicious code;

- Business continuity plans for e-banking services including alternate processing lines, backup servers, emergency operating procedures, etc.;
- Performance of, and access to, vulnerability assessments, penetration tests, and financial and operations audits;Limitations on subcontracting of services, either domestically or internationally;
- Choice of law and jurisdiction for dispute resolution and access to information by the financial institution and its regulators; and
- For foreign-based vendors or service providers (i.e., country of residence is different from that of the institution), in addition to the above items, contract options triggered by increased risks due to adverse economic or political developments in the vendor's or service provider's home country.

Oversight and Monitoring of Third Parties

Financial institutions that outsource e-banking technical support must provide sufficient oversight of service providers' activities to identify and control the resulting risks. The key to good oversight typically lies in effective MIS. However, for MIS to be effective the financial institution must first establish clear performance expectations. Wherever possible, these expectations should be clearly documented in the service contract or an addendum to the contract. Effective and timely MIS can alert the serviced institution to developing service, financial or security problems at the vendor - problems that might require execution of contingency plans supporting a change in vendor or in the existing service relationship.

The type and frequency of monitoring reports needed varies, depending on the complexity of the services provided and the division of responsibilities between the institution and its service provider(s). Service providers can build MIS capabilities into the administrative modules of their application, provide on-line reports, or they can provide periodic written reports. Some examples of items that might be tracked by e-banking monitoring reports are listed below:

E-banking service availability. Reports might include statistics regarding the frequency and duration of service disruptions, including the reasons for any service disruptions (maintenance, equipment/network problems, security incidents, etc.); "up time" and "down time" percentages for website and e-banking services; and volume and type of website access problems reported by e-banking customers.

Activity levels and service volumes. Reports might include number of accounts serviced, number and percentage of new, active, or inactive accounts; breakdown of intrabank transfers by number, dollar size, and account type; bill payment activity by number, average dollar, and recurring versus one-time payments; volume of associated ACH returns and rejects, fee breakdown by source and type; and activity on informational website usage by webpages viewed.

Performance efficiency. Reports might include average response times by time of day (including complaints about slow response); bill payment activity by check versus ACH; server capacity utilization; customer service contacts by type of inquiry and average time to resolution; and losses from errors, fraud, or repudiated items.

Security incidents. Reports might include volume of rejected log-on attempts, password resets, attempted and successful penetration attempts, number and type of trapped viruses or other malicious code, and any physical security breaches.

Vendor stability. Reports might include quarterly or annual financial reports, number of new or departing customers, changes in systems or equipment, and employee turnover statistics, including any changes in management positions.

Quality Assurance. Reports on performance, audit results, penetration tests, and vulnerability assessments, including servicer actions to address any identified deficiencies.

Information Security Program

Action Summary

E-banking introduces information security risk management challenges. Financial institution directors and senior management should ensure the information security program addresses these challenges and takes the appropriate actions.

- Ensure compliance with the "Guidelines Establishing Standards for Safeguarding Customer Information" (as issued pursuant to section 501(b) of the Gramm-Leach-Bliley Act of 1999 (GLBA).
- Ensure the institution has the appropriate security expertise for its e-banking platform.
- Implement security controls sufficient to manage the unique security risks confronting the institution. Control considerations include:
    - Ongoing awareness of attack sources, scenarios, and techniques;
    - Up-to-date equipment inventories and network maps;
    - Rapid identification and mitigation of vulnerabilities;
    - Network access controls over external connections;
    - Hardened systems with unnecessary or vulnerable services or files disabled or removed;
    - Use of intrusion detection tools and intrusion response procedures;
    - Physical security of all e-banking computer equipment and media; and
    - Baseline security settings and usage policies for employees accessing the e-banking system or communicating with customers.
- Use verification procedures sufficient to adequately identify the individual asking

to conduct business with the institution.

- Use authentication methods sufficient to verify individuals are authorized to use the institution's systems based on the sensitivity of the data or connected systems.
- Develop policies for notifying customers in the event of a security breach effecting their confidential information.
- Monitor and independently test the effectiveness of the institution's security program.

Information security is essential to a financial institution's ability to deliver e-banking services, protect the confidentiality and integrity of customer information, and ensure that accountability exists for changes to the information and the processing and communications systems. Depending on the extent of in-house technology, a financial institution's e-banking systems can make information security complex with numerous networking and control issues. The IT Handbook's "Information Security Booklet" addresses security in much greater detail. Refer to that booklet for additional information on security and to supplement the examination coverage in this booklet.

Security Guidelines

Financial institutions must comply with the "Guidelines Establishing Standards for Safeguarding Customer Information" (guidelines) as issued pursuant to the Gramm-Leach-Bliley Act of 1999 (GLBA).The guidelines were published in the Federal Register on February 1, 2001, and effective on July 1, 2001. When financial institutions introduce e-banking or related support services, management must re-assess the impact to customer information under the GLBA. The guidelines require financial institutions to:

- Ensure the security and confidentiality of customer information;
- Protect against any anticipated threats or hazards to the security or integrity of such information; and
- Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.

The guidelines outline specific measures institutions should consider in implementing a security program. These measures include:

- Identifying and assessing the risks that may threaten consumer information;In order to perform a risk assessment, a financial institution gathers information about the internal and external environment, analyzes that information, and provides a hierarchical list of risks to be mitigated. This assessment guides the testing program, indicating which controls should be subject to more frequent or rigorous testing.
- Developing a written plan containing policies and procedures to manage and ontrol these risks;
- Implementing and testing the plan; and
- Adjusting the plan on a continuing basis to account for changes in technology, the sensitivity of customer information, and internal or external threats to information security.

The guidelines also outline the responsibilities of management to oversee the protection of customer information including the security of customer information maintained or processed by service providers. Oversight of third-party service providers and vendors is discussed in this booklet under the headings "Board and Management Oversight" and "Managing Outsourcing Relationships." Additional information on the guidelines can be found in the IT Handbook's "Management Booklet." The IT Handbook's "Information Security Booklet" presents additional information on the risk assessment process and information processing controls.

The guidelines required by the GLBA apply to customer information stored in electronic form as well as paper-based records. Examination procedures specifically addressing compliance with the GLBA guidelines can be accessed through the agency websites listed in the reference section of this booklet. Although the guidelines supporting GLBA define customer as "a consumer who has a customer relationship with the institution," management should consider expanding the written information security program to cover the institution's own confidential records as well as confidential information about its commercial customers.

Information Security Controls

Security threats can affect a financial institution through numerous vulnerabilities. No single control or security device can adequately protect a system connected to a public network. Effective information security comes only from establishing layers of various control, monitoring, and testing methods. While the details of any control and the effectiveness of risk mitigation depend on many factors, in general, each financial institution with external connectivity should ensure the following controls exist internally or at their TSP.

- Ongoing knowledge of attack sources, scenarios, and techniques. Financial institutions should maintain an ongoing awareness of attack threats through membership in information-sharing entities such as the Financial Services - Information Sharing and Analysis Center (FS-ISAC), Infragard, the CERT Coordination Center, private mailing lists, and other security information sources. All defensive measures are based on knowledge of the attacker's capabilities and goals, as well as the probability of attack.

- Up-to-date equipment inventories, and network maps. Financial institutions should have inventories of machines and software sufficient to support timely security updating and audits of authorized equipment and software. In addition, institutions should understand and document the connectivity between various network components including remote users, internal databases, and gateway servers to third parties. Inventories of hardware and the software on each system can accelerate the institution's response to newly discovered vulnerabilities and support the proactive identification of unauthorized devices or software.

- Rapid response capability to react to newly discovered vulnerabilities. Financial institutions should have a reliable process to become aware of new vulnerabilities and to react as necessary to mitigate the risks posed by newly discovered vulnerabilities. Software is seldom flawless. Some of those flaws may represent security vulnerabilities, and the financial institution may need to correct the software code using temporary fixes, sometimes called a "patch." In some cases, management may mitigate the risk by reconfiguring other computing devices. Frequently, the financial institution must respond rapidly, because a widely known vulnerability is subject to an increasing number of attacks.

- Network access controls over external connections. Financial institutions should carefully control external access through all channels including remote dial-up, virtual private network connections, gateway servers, or wireless access points. Typically, firewalls are used to enforce an institution's policy over traffic entering the institution's network. Firewalls are also used to create a logical buffer, called a "demilitarized zone," or DMZ, where servers are placed that receive external traffic. The DMZ is situated between the outside and the internal network and prevents direct access between the two. Financial institutions should use firewalls to enforce policies regarding acceptable traffic and to screen the internal network from directly receiving external traffic.

- System hardening. Financial institutions should "harden" their systems prior to placing them in a production environment. Computer equipment and software are frequently shipped from the manufacturer with default configurations and passwords that are not sufficiently secure for a financial institution environment. System "hardening" is the process of removing or disabling unnecessary or insecure services and files. A number of organizations have current efforts under way to develop security benchmarks for various vendor systems. Financial institutions should assess their systems against these standards when available.

- Controls to prevent malicious code. Financial institutions should reduce the risks posed by malicious code by, among other things, educating employees in safe computing practices, installing anti-virus software on servers and desktops, maintaining up-to-date virus definition files, and configuring their systems to protect against the automatic execution of malicious code. Malicious code can deny or degrade the availability of computing services; steal, alter, or insert information; and destroy any potential evidence for criminal prosecution. Various types of malicious code exist including viruses, worms, and scripts using active content.

- Rapid intrusion detection and response procedures. Financial institutions should have mechanisms in place to reduce the risk of undetected system intrusions. Computing systems are never perfectly secure. When a security failure occurs and an attacker is "in" the institution's system, only rapid detection and reaction can minimize any damage that might occur. Techniques used to identify intrusions include intrusion detection systems (IDS) for the network and individual servers (i.e., host computer), automated log correlation and analysis, and the identification and analysis of operational anomalies.

- Physical security of computing devices. Financial institutions should mitigate the risk posed by unauthorized physical access to computer equipment through such techniques as placing servers and network devices in areas that are available only to specifically authorized personnel and restricting administrative access to machines in those limited access areas. An attacker's physical access to computers and network devices can compromise all other security controls. Computers used by vendors and employees for remote access to the institution's systems are also subject to compromise. Financial institutions should ensure these computers meet security and configuration requirements regardless of the controls governing remote access.

- User enrollment, change, and termination procedures. Financial institutions should have a strong policy and well-administered procedures to positively identify authorized users when given initial system access (enrollment) and, thereafter, to limit the extent of their access to that required for business purposes, to promptly increase or decrease the degree of access to mirror changing job responsibilities, and to terminate access in a timely manner when access is no longer needed.

- Authorized use policy. Each financial institution should have a policy that addresses the systems various users can access, the activities they are authorized to perform, prohibitions against malicious activities and unsafe computing practices, and consequences for noncompliance. All internal system users and contractors should be trained in, and acknowledge that they will abide by, rules that govern their use of the institution's system.

- Training. Financial institutions should have processes to identify, monitor, and address training needs. Each financial institution should train their personnel in the technologies they use and the institution's rules governing the use of that technology. Technical training is particularly important for those who oversee the key technology controls such as firewalls, intrusion detection, and device configuration. Security awareness training is important for all users, including the institution's e-banking customers.

- Independent testing. Financial institutions should have a testing plan that identifies control objectives; schedules tests of the controls used to meet those objectives; ensures prompt corrective action where deficiencies are identified; and provides independent assurance for compliance with security policies. Security tests are necessary to identify control deficiencies. An effective testing plan identifies the key controls, then tests those controls at a frequency based on the risk that the control is not functioning. Security testing should include independent tests conducted by personnel without direct responsibility for security administration. Adverse test results indicate a control is not functioning and cannot be relied upon. Follow-up can include correction of the specific control, as well as a search for, and correction of, a root cause. Types of tests include audits, security assessments, vulnerability scans, and penetration tests.

Authenticating E-Banking Customers

E-banking introduces the customer as a direct user of the institution's technology. Customers have to log on and use the institution's systems. Accordingly, the financial institution must control their access and educate them in their security responsibilities. While authentication controls play a significant role in the internal security of an organization, this section of the booklet discusses authentication only as it relates to the e-banking customer.FFIEC Guidance: Authentication in an Electronic Banking Environment (July 30, 2001). See the corresponding agency issuances in appendix C.

Authenticating New Customers

Verifying a customer's identity, especially that of a new customer, is an integral part of all financial services. Consistent with the USA PATRIOT Act, federal regulations require that by October 1, 2003, each financial institution must develop and implement a customer identification program (CIP) that is appropriate given the institution's size, location and type of business.See 68 Federal Register 25090 (May 9, 2003); 12 CFR Part 21 (OCC); 12 CFR Parts 208 and 211 (Board); 12 CFR Part 326 (FDIC); 12 CFR Part 563 (OTS), and 12 CFR 748 (NCUA). The CIP must be written, incorporated into the institution's Bank Secrecy Act/Anti-Money Laundering program, and approved by the institution's board of directors. The CIP must include risk-based procedures to verify the identity of customers (generally persons opening new accounts). Procedures in the program should describe how the bank will verify the identity of the customer using documents, nondocumentary methods, or a combination of both. The procedures should reflect the institution's account opening processes - whether face-to-face or remotely as part of the institution's e-banking services.

As part of its nondocumentary verification methods, a financial institutions may rely on third parties to verify the identity of an applicant or assist in the verification. The financial institution is responsible for ensuring that the third party uses the appropriate level of verification procedures to confirm the customer's identity. New account applications submitted on-line increase the difficulty of verifying the application information. Many institutions choose to require the customer to come into an office or branch to complete the account opening process. Institutions conducting the entire account opening process through the mail or on-line should consider using third-party databases to provide:

- Positive verification to ensure that material information provided by an applicant matches information available from third-party sources,
- Logical verification to ensure that information provided is logically consistent, and
- Negative verification to ensure that information provided has not previously been associated with fraudulent activity (e.g., an address previously associated with a fraudulent application).

Authenticating Existing Customers

In addition to the initial verification of customer identities, the financial institution must also authenticate its customers' identities each time they attempt to access their confidential on-line information. The authentication method a financial institution chooses to use in a specific e-banking application should be appropriate and "commercially reasonable" in light of the risks in that application. Whether a method is a commercially reasonable system depends on an evaluation of the circumstances. Financial institutions should weigh the cost of the authentication method, including technology and procedures, against the level of protection it affords and the value or sensitivity of the transaction or data to both the institution and the customer. What constitutes a commercially reasonable system may change over time as technology and standards evolve.

Authentication methods involve confirming one or more of three factors:

- Something only the user should know, such as a password or PIN;
- Something the user possesses, such as an ATM card, smart card, or token; or
- Something the user is, such as a biometric characteristic like a fingerprint or iris pattern.

Authentication methods that depend on more than one factor are typically more difficult to compromise than single-factor systems therefore suggesting a higher reliability of authentication. For example, the use of a customer ID and password is considered single-factor authentication since both items are something the user knows. A common example of two-factor authentication is found in most ATM transactions where the customer is required to provide something the user possesses (i.e., the card) and something the user knows (i.e., the PIN). Single factor authentication alone may not be adequate for sensitive communications, high dollar value transactions, or privileged user access (i.e., network administrators). Multi-factor techniques may be necessary in those cases. Institutions should recognize that a single factor system may be "tiered" (e.g., require multiple passwords) to enhance security without the implementation of a true two-factor system.A "tiered" single factor authentication system would include the use of multiple levels of a single factor (e.g., the use of two or more passwords or PINs employed at different points in the authentication process). Tiering may not be as strong as two-factor authentication because the means used to steal the first password may be equally effective against the second password.

Password Administration

Despite the concerns regarding single-factor authentication, many e-banking services still rely on a customer ID and password to authenticate an existing customer. Some security professionals criticize passwords for a number of reasons including the need for passwords whose strength places the password beyond the user's ability to comply with other password policies such as not writing the password down. Password-cracking software and log-on scripts can frequently guess passwords regardless of the use of encryption. Popular acceptance of this form of authentication rests on its ease of use and its adaptability within existing infrastructures.

Financial institutions that allow customers to use passwords with short character length, readily identifiable words or dates, or widely used customer information (e.g., Social Security numbers) may be exposed to excessive risks in light of the security threats from hackers and fraudulent insider abuse. Stronger security in password structure and implementation can help mitigate these risks. Another way to mitigate the risk of scripted attacks is to make the user ID more random and not based on any easily determined format or commonly available information. There are three aspects of passwords that contribute to the security they provide: password secrecy, password length and composition, and administrative controls.

Password secrecy. The security provided by password-only systems depends on the secrecy of the password. If another party obtains the password, he or she can perform the same transactions as the intended user. Passwords can be compromised because of customer behavior or techniques that capture passwords as they travel over the Internet. Attackers can also use well-known weaknesses to gain access to a financial institution's (or its service provider's) Internet-connected systems and obtain password files. Because of these vulnerabilities, passwords and password files should be encrypted when stored or transmitted over open networks such as the Internet. The system should prohibit any user, including the system or security administrator, from printing or viewing unencrypted passwords. In addition, security administrators should ensure password files are protected and closely monitored for compromise because if stolen an attacker may be able to decrypt an encrypted password file.

Financial institutions need to emphasize to customers the importance of protecting the password's confidentiality. Customers should be encouraged to log off unattended computers that have been used to access on-line banking systems especially if they used public access terminals such as in a library, institution lobby, or Internet cafe.

Password length and composition. The appropriate password length and composition depends on the value or sensitivity of the data protected by the password and the ability of the user to maintain the password as a shared secret. Common identification items - for example, dictionary words, proper names, or social security numbers - should not be used as passwords. Password composition standards that require numbers or symbols in the sequence of a password, in conjunction with both upper and lower case alphabetic characters, provide a stronger defense against password-cracking programs. Selecting letters that do not create a common word but do create a mnemonic - for example the first letter of each word in a favorite phrase, poem, or song - can create a memorable password that is difficult to crack.

Systems linked to open networks, like the Internet, are subject to a greater number of individuals who may attempt to compromise the system. Attackers may use automated programs to systematically generate millions of alphanumeric combinations to learn a customer's password (i.e., "brute force" attack). A financial institution can reduce the risk of password compromise by communicating and enforcing prudent password selection, providing guidance to customers and employees, and careful protection of the password file.

Password administration controls. When evaluating password-based e-banking systems, management should consider whether the authentication system's control capabilities are consistent with the financial institution's security policy. This includes evaluating such areas as password length and composition requirements, incorrect log-on lockout, password expiration, repeat password usage, and encryption requirements, as well as the types of activity monitoring and exception reports in use.

Each financial institution must evaluate the risks associated with its authentication methods given the nature of the transactions and information accessed. Financial institutions that assess the risk and decide to rely on passwords, should implement strong password administration standards.

Administrative controls

Action Summary

E-banking presents new administrative control requirements and potentially increases the importance of existing controls. Management must evaluate its administrative controls to maximize the availability and integrity of e-banking systems. E-banking information can support identity theft for either fraud at the subject institution or for creating fraudulent accounts at other institutions. Institutions should consider the adequacy of the following controls:

- Segregation of e-banking duties to minimize the opportunity for employee fraud;
- Dual-control procedures especially for sensitive functions like encryption key retrieval or large on-line transfers;
- Reconcilement of e-banking transactions;
- Suspicious activity reviews and fraud detection with targeted review of unusually large transaction amounts or volumes;
- Periodic monitoring to detect websites with similar names, possibly established for fraudulent purposes;
- Error checks and customer guidance to prevent unintentional errors;
- Alternate channel confirmations to ensure account activity or maintenance changes are properly authorized; and
- Business disruption avoidance strategies and recovery plans.

E-banking activities are subject to the same risks as other banking processes. However, the processes used to monitor and control these risks may vary because of e-banking's heavy reliance on automated systems and the customer's direct access to the institution's computer network. Some of the controls that help assure the integrity and availability of e-banking systems are discussed below.

Internal Controls

Segregation of duties. E-banking support relies on staff in the service provider's operations or staff in the institution's bookkeeping, customer service, network administration, or information security areas. However, no one employee should be able to process a transaction from start to finish. Institution management must identify and mitigate areas where conflicting duties create the opportunity for insiders to commit fraud. For example, network administrators responsible for configuring servers and firewalls should not be the only ones responsible for checking compliance with security policies related to network access. Customer service employees with access to confidential customer account information should not be responsible for daily reconcilements of e-banking transactions.

Dual controls. Some sensitive transactions necessitate making more than one employee approve the transaction before authorizing the transaction. Large electronic funds transfers or access to encryption keys are examples of two e-banking activities that would typically warrant dual controls.

Reconcilements. E-banking systems should provide sufficient accounting reports to allow employees to reconcile individual transactions to daily transaction totals.

Suspicious activity. Financial institutions should establish fraud detection controls that could prompt additional review and reporting of suspicious activity. Some potential concerns to consider include false or erroneous application information, large check deposits on new e-banking accounts, unusual volume or size of funds transfers, multiple new accounts with similar account information or originating from the same Internet address, and unusual account activity initiated from a foreign Internet address. Security- and fraud-related events may require the filing of a SAR with the Financial Crimes Enforcement Network (FinCEN).

Similar website names. Financial institutions should exercise care in selecting their website name(s) in order to reduce possible confusion with those of other Internet sites. Institutions should periodically scan the Internet to identify sites with similar names and investigate any that appear to be posing as the institution. Suspicious sites should be reported to appropriate criminal and regulatory authorities.

Error checks. E-banking activities provide limited opportunities for customers to ask questions or clarify their intentions regarding a specific transaction. Institutions can reduce customer confusion and the potential for unintended transactions by requiring written contracts explaining rights and responsibilities, by providing clear disclosures and on-line instructions or help functions, and by incorporating proactive confirmations into the transaction initiation process.

On-line instructions, help features, and proactive confirmations are typically part of the basic design of an e-banking system and should be evaluated as part of the initial due diligence process. On-line forms can include error checks to identify common mistakes in various fields. Proactive confirmations can require customers to confirm their actions before the transaction is accepted for processing. For example, a bill payment customer would enter the amount and date of payment and specify the intended recipient. But, before accepting the customer's instructions for processing, the system might require the customer to review the instructions entered and then confirm the instruction's accuracy by clicking on a specific box or link.

Alternate channel confirmations. Financial institutions should consider the need to have customers confirm sensitive transactions like enrollment in a new on-line service, large funds transfers, account maintenance changes, or suspicious account activity. Positive confirmations for sensitive on-line transactions provide the customer with the opportunity to help catch fraudulent activity. Financial institutions can encourage customer participation in fraud detection and increase customer confidence by sending confirmations of certain high-risk activities through additional communication channels such as the telephone, e-mail, or traditional mail.

Business Continuity Controls

E-banking customers often expect 24-hour availability. Service interruptions can significantly affect customers if the institution offers more than the most basic services. For example, customer bill payment transactions may not be paid on time. Due to the potential impact on customers and customer service, financial institutions should analyze the impact of service outages and take steps to decrease the probability of outages and minimize the recovery time if one should occur. Some considerations include:

- Conducting a business impact analysis of e-banking services that defines the minimum level of service required and establishes recovery-time objectives;Building redundancy into critical network components to avoid single points of failure;
- Updating business continuity plans to address e-banking;
- Developing customer communication plans prior to an outage;
- Reviewing the compatibility of key third parties' business continuity plans; and
- Periodically testing business resumption capabilities to determine if objectives can be met.

Based on activity volumes, number of customer effected, and the availability of alternate service channels (branches, checks, etc.), some institutions may not consider e-banking services as "mission critical" warranting a high priority in its business continuity plan. Management should periodically reassess this decision to ensure the supporting rationale continues to reflect actual growth and expansion in e-banking services.

Legal and Compliance Issues

Action Summary

Because e-banking limits face-to-face interaction and the paper-based exchange of information with customers, e-banking introduces new compliance or legal risks. Institutions should:

- Clearly identify the official name of the financial institution providing the e-banking services;
- Properly disclose their customer privacy and security policies on their websites; and
- Ensure that advertisements, notices, and disclosures are in compliance with

applicable statutes and regulations, including the E-Sign Act.

Financial institutions should comply with all legal requirements relating to e-banking, including the responsibility to provide their e-banking customers with appropriate disclosures and to protect customer data. Failure to comply with these responsibilities could result in significant compliance, legal, or reputation risk for the financial institution.

Trade Names on the Internet

Financial institutions may choose to use a name different from their legal name for their e-banking operations. Since these trade names are not the institution's official corporate title, information on the website should clearly identify the institution's legal name and physical location. This is particularly important for websites that solicit deposits since persons may inadvertently exceed deposit insurance limits. The risk management techniques financial institutions should use are based on an "Interagency Statement for Branch Names" issued May 1, 1998.

Financial institutions that use trade names for e-banking operations should:

- Disclose clearly and conspicuously, in signs, advertising, and similar materials that the facility is a division or operating unit of the insured institution;
- Use the legal name of the insured institution for legal documents, certificates of deposit, signature cards, loan agreements, account statements, checks, drafts, and other similar documents; and
- Train staff of the insured institution regarding the possibility of customer confusion with respect to deposit insurance.

Disclosures must be clear, prominent, and easy to understand. Examples of how Internet disclosures may be made conspicuous include using large font or type that is easily viewable when a page is first opened; inserting a dialog page that appears whenever a customer accesses a webpage; or placing a simple graphic near the top of the page or in close proximity to the financial institution's logo. These examples are only some of the possibilities for conspicuous disclosures given the available technology. Front-line employees (e.g., call center staff) should be trained to ensure that customers understand these disclosures and mitigate confusion associated with multiple trade names.

Website Content

Financial institutions can take a number of steps to avoid customer confusion associated with their website content. Some examples of information a financial institution might provide to its customers on its website include:

- The name of the financial institution and the location of its main office (and branch offices if applicable);
- The identity of the primary financial institution supervisory authority responsible for the supervision of the financial institution's main office;
- Instructions on how customers can contact the financial institution's customer service center regarding service problems, complaints, suspected misuse of accounts, etc.;
- Instructions on how to contact the applicable supervisor to file consumer complaints; and
- Instructions for obtaining information on deposit insurance coverage and the level of protection that the insurance affords, including links to the FDIC or NCUA websites at http://www.fdic.gov or www.ncua.gov, respectively.

Customer Privacy and Confidentiality

Maintaining the privacy of a customer's information is one of the cornerstones upon which trust in the U.S. banking system is based. Misuse or unauthorized disclosure of confidential customer data may expose a financial institution to customer litigation or action by regulatory agencies. To meet expectations regarding the privacy of customer information, financial institutions should ensure that their privacy policies and standards comply with applicable privacy laws and regulations, particularly the privacy requirements established by GLBA. The regulation implementing GLBA's requirements also describes standards on electronic disclosures that apply if an institution elects to display its privacy policy on its website.

Transaction Monitoring and Consumer Disclosures

The general requirements and controls that apply to paper-based transactions also apply to electronic financial services. Consumer financial services regulations generally require that institutions send, provide, or deliver disclosures to consumers as opposed to merely making the disclosures available. Financial institutions are permitted to provide such disclosures electronically if they obtain consumers' consent in a manner consistent with the requirements of the federal Electronic Signatures in Global and National Commerce Act (the E-Sign Act). The Federal Reserve Board has issued interim rules providing guidance on how the E-Sign Act applies to the consumer financial services and fair lending laws and regulations administered by the Board.66 Federal Register 17,779 (April 4, 2001) (Regulation B, Equal Credit Opportunity); 66 Federal Register 17.786 (April 4, 2001) (Regulation E, Electronic Fund Transfers); 66 Federal Register. 17,795 (April 4, 2001) (Regulation DD, Truth in Savings); 66 Federal Register 17,322 (March 30, 2001) (Regulation M, Consumer Leasing); 66 Federal Register 17,329 (March 30, 2001) (Regulation Z, Truth in Lending). However mandatory compliance with the interim rules was not required at the time of this booklet's publication.66 Federal Register 41,439 (August 8, 2001) (lifting mandatory compliance date). Financial institutions may provide electronic disclosures under their existing policies or practices, or may follow the interim rules, until the Board issues permanent rules.

When disclosures are required to be in writing, the E-Sign Act requires that financial institutions generally must obtain a consumer's affirmative consent to provide disclosures electronically. Under the E-Sign Act, a consumer must among other things provide such consent electronically and in a manner that reasonably demonstrates that he or she can access the electronic record in the format used by the institution. In addition, the institution must advise customers of their right to withdraw their consent for electronic disclosures and explain any conditions, consequences, or fees triggered by withdrawing such consent.

Additional information on consumer regulatory requirements can be found in this booklet's "Compliance/Legal Risk" section and on each agency's website.

Endnotes

[1] Under the Electronic Signatures in Global and National Commerce Act, Pub. L. 106-229, (E-SIGN Act), to obtain effective consumer consent to receiving electronic disclosures, financial institutions must among other things inform consumers of the hardware and software requirements for retention of electronic records that will be provided as disclosures. 15 USC 7001(c)(1)(B). This requirement should be carefully considered by institutions whose customers wish to use wireless devices with limited storage as their primary access device.

[2] The Act specifically provides that an oral communication will not qualify as an "electronic record." 15 USC 7001(c)(6). The treatment of voice recognition technology under this provision is uncertain.

Appendix A: Examination Procedures

Introduction

The examiner's primary goal in reviewing e-banking activities is to determine whether the institution is providing e-banking products and services in a safe and sound manner that supports compliance with consumer-protection regulations. This determination is based on whether the institution's risk management practices are commensurate with the level of risk in its e-banking activities.

The e-banking examination procedures are a tool to help examiners reach conclusions regarding the effectiveness of an institution's risk management of e-banking activities. **Examiners should use their judgment, consistent with the institution's supervisory strategy, in selecting applicable examination objectives and determining the need for specific testing of controls**. Examiners may rely on the work of auditors and consultants deemed independent and competent in establishing their examination scope.

The examination procedures that follow focus on the risks inherent in the processes and technologies supporting e-banking products and services. They supplement, but do not replace, procedures from other IT Handbook booklets that apply to general IT activities (e.g., program development and maintenance, networking, information security, etc.). Depending on the scope of coverage targeted, examiners should consider using these procedures in combination with others from the IT Handbook and related issuances.

The structure of the e-banking examination procedures parallels the structure of the narrative portion of this booklet. The procedures cover:

- Setting the examination scope,
- Evaluating board and management oversight,
- Assessing the information security program,
- Reviewing legal and compliance issues, and
- Deriving exam conclusions.

Depending on the complexity of the institution's activities and the scope of prior reviews, it is generally not necessary to complete all of the examination objectives or procedures in order to reach conclusions on the effectiveness of the financial institution's risk management processes. The procedures are designed for conducting targeted, integrated reviews of new or significantly expanded e-banking services. However, for follow-up activities or e-banking reviews conducted as part of a comprehensive review of an institution's IT activities, examiners should customize their e-banking coverage to avoid duplication of topics covered in other examination programs.

This section of the booklet also includes discussion points examiners can use as a reference when talking to management as they are considering or implementing e-banking products and services and a sample list of items to include in the request letter for each of the objectives stated in the examination procedures.

Discussion Points for Examiners

Financial institutions frequently contact examiners seeking guidance on things to consider when they plan to offer or expand e-banking services. The following discussion points are offered as a guide to assist examiners when discussing e-banking plans and strategies with institution management.

Strategic Plans - Decisions on e-banking should be consistent with the financial institution's strategic and operating business plans. Any decision to offer or expand e-banking services should consider customer demand for the services, competitive issues, and the risks in the technology. The institution should periodically evaluate the success of its e-banking strategy and make changes as appropriate.

Impact on Earnings and Capital - Financial institution management should have realistic projections of the expected impact of e-banking on earnings and capital. If management projects a significant impact then profitability plans should address pricing and marketing expenses. If management projects rapid growth in loans or deposits, then plans should address the impact on liquidity, asset quality, and capital adequacy.

E-Banking Software and Service Provider Selection - Financial institutions should provide an appropriate level of due diligence in selecting third-party providers or developing systems in-house. User departments should be involved in the selection process since they will work with the system on a daily basis once it is operational.

Security - Financial institution management should understand security issues associated with e-banking. Security issues include customer verification and authentication, data confidentiality and integrity, and intrusion prevention and detection. Management should measure the effectiveness of security controls.

Internal Controls and Audit - The institution's board and management should ensure that internal control and audit processes are adequate to enable the identification, measurement, and monitoring of the risks associated with e-banking. Management should attempt to quantify increased expenses and losses due to internal control-related weaknesses and fraud.

Legal Requirements - Management should research and understand various legal requirements, including compliance issues, as part of the e-banking decision process. Many legal issues are evolving and will require management to monitor developments.

Vendor Management - Research of outsourcing arrangements should include consideration of potential vendors' financial condition, reputation and expertise, years in business, history of service interruptions and recoveries, and future business plans. Selection should also consider the ability to agree on a contract that clearly defines responsibility for maintaining and sharing information and any resulting liability for its unauthorized use or disclosure.

Business Continuity Planning - Whether provided by the financial institution or a third party, management should plan for recovery of critical e-banking technology and business functions and develop alternate operating processes for use during service disruptions.

Insurance - A review of insurance coverage may be in order to determine if existing policies specifically cover or exclude activities conducted over open networks like the Internet.

Expertise - The financial institution should ensure it has the proper level of expertise to make business decisions regarding e-banking and network security. The board of directors and senior management may need to enhance their understanding of technology issues. If such expertise is not available in-house, the institution should consider engaging outside expertise.

General Procedures

Objective 1: Determine the scope for the examination of the institution's e-banking activities consistent with the nature and complexity of the institution's operations.

spacer

1. Review the following documents to identify previously noted issues related to the e-banking area that require follow-up:

- Previous regulatory examination reports
- Supervisory strategy
- Follow-up activities
- Work papers from previous examinations
- Correspondence

2. Identify the e-banking products and services the institution offers, supports, or provides automatic links to (i.e., retail, wholesale, investment, fiduciary, e-commerce support, etc.).

3. Assess the complexity of these products and services considering volumes (transaction and dollar), customer base, significance of fee income, and technical sophistication.

4. Identify third-party providers and the extent and nature of their processing or support

services.

5. Discuss with management or review MIS or other monitoring reports to determine the institution's recent experience and trends for the following:

- Intrusions, both attempted and successful;
- Fraudulent transactions reported by customers;
- Customer complaint volumes and average time to resolution; and
- Frequency and duration of service disruptions.

6. Review audit and consultant reports, management's responses, and problem tracking systems to identify potential issues for examination follow-up. Possible sources include:

- Internal and external audit reports and SSAE-16 Attestation reports and reviews for service providers,
- Security reviews/evaluations from internal risk review or external consultants (includes vulnerability and penetration testing), and
- Findings from GLBA security and control tests and annual GLBA reports to the board.

7. Review network schematic to identify the location of major e-banking components. Document the location and the entity responsible for development, operation, and support of each of the major system components.

8. Review the institution's e-banking site(s) to gain a general understanding of the scope of e-banking activities and the website's organization, structure, and operability.

9. Discuss with management recent and planned changes in:

- The types of products and services offered;
- Marketing or pricing strategies;
- Network structure;
- Risk management processes, including monitoring techniques;

- Policies, processes, personnel, or controls, including strategies for intrusion responses or business continuity planning;
- Service providers or other technology vendors; and
- The scope of independent reviews or the individuals or entities conducting them.

10. Based on the findings from the previous steps, determine the scope of the e-banking review. Discuss, as appropriate, with the examiner or office responsible for supervisory oversight of the institution.

Select from among the following examination objectives and procedures those that are appropriate to the examination's scope. When more in-depth coverage of an area is warranted, examiners should select procedures from other booklets of the IT Handbook as necessary (e.g., "Information Security Booklet," "Retail Payments Systems Booklet," etc.). For more complex e-banking environments, examiners may need to integrate IT coverage with business line-specific coverage. In those cases, examiners should consult other subject matter experts and consider inclusion of the member agency's expanded procedures (e.g., compliance, retail lending, fiduciary/asset management, etc.).

BOARD AND MANAGEMENT OVERSIGHT

Objective 2: Determine the adequacy of board and management oversight of e-banking activities with respect to strategy, planning, management reporting, and audit.

1. Evaluate the institution's short- and long-term strategies for e-banking products and services. In assessing the institution's planning processes, consider whether:

- The scope and type of e-banking services are consistent with the institution's overall mission, strategic goals, operating plans, and risk tolerance;
- The institution's MIS is adequate to measure the success of e-banking strategies based on clearly defined organizational goals and objectives;
- Management's understanding of industry standards is sufficient to ensure compatibility with legacy systems;
- Cost-benefit analyses of e-banking activities consider the costs of start-up, operation, administration, upgrades, customer support, marketing, risk management, monitoring, independent testing, and vendor oversight (if applicable);
- Management's evaluation of security risks, threats, and vulnerabilities is realistic and consistent with institution's risk profile;

- Management's knowledge of federal and state laws and regulations as they pertain to e-banking is adequate; and
- A process exists to periodically evaluate the institution's e-banking product mix and marketing successes and link those findings to its planning process.

2. Determine whether e-banking guidance and risk considerations have been incorporated into the institution's operating policies to an extent appropriate for the size of the financial institution and the nature and scope of its e-banking activities. Consider whether the institution's policies and practices:

- Include e-banking issues in the institution's processes and responsibilities for identifying, measuring, monitoring, and controlling risks;
- Define e-banking risk appetite in terms of types of product or service, customer restrictions (local/domestic/foreign), or geographic lending territory;
- Consider, if appropriate, e-banking activities as a mission-critical activity for business continuity planning;
- Assign day-to-day responsibilities for e-banking compliance issues including marketing, disclosures, and BSA/OFAC issues;
- Require e-banking issues to be included in periodic reporting to the board of directors on the technologies employed, risks assumed, and compensating risk management practices;
- Maintain policies and procedures over e-commerce payments (i.e., bill payment or cash management) consistent with the risk and controls associated with the underlying payment systems (check processing, ACH, wire transfers, etc.);
- Establish policies to address e-commerce support services (aggregation, certificate authority, commercial website hosting/design, etc.);
- Include e-banking considerations in the institution's written privacy policy; and
- Require the board of directors to periodically review and approve updated policies and procedures related to e-banking.

3. Assess the level of oversight by the board and management in ensuring that planning and monitoring are sufficiently robust to address heightened risks inherent in e-banking products and services. Consider whether:

- The board reviews, approves, and monitors e-banking technology-related projects that may have a significant impact on the financial institution's risk profile;
- The board ensures appropriate programs are in place to oversee security, recovery, and third-party providers of critical e-banking products and services;

- Senior management evaluates whether technologies and products are in line with the financial institution's strategic goals and meet market needs;
- Senior management periodically evaluates e-banking performance relative to original/revised project plans;
- Senior management has developed, as appropriate, exit strategies for high-risk activities; and
- Institution personnel have the proper skill sets to evaluate, select, and implement e-banking technology.

4. Evaluate adequacy of key MIS reports to monitor risks in e-banking activities. Consider monitoring of the following areas:

- Systems capacity and utilization;
- Frequency and duration of service interruptions;
- Volume and type of customer complaints, including time to successful resolution;
- Transaction volumes by type, number, dollar amount, behavior (e.g., bill payment or cash management transaction need sufficient monitoring to identify suspicious or unusual activity);
- Exceptions to security policies whether automated or procedural;
- Unauthorized penetrations of e-banking system or network, both actual and attempted;
- Losses due to fraud or processing/balancing errors; and
- Credit performance and profitability of accounts originated through e-banking channels.

5. Determine whether audit coverage of e-banking activities is appropriate for the type of services offered and the level of risk assumed. Consider the frequency of e-banking reviews, the adequacy of audit expertise relative to the complexity of e-banking activities, the extent of functions outsourced to third-party providers. The audit scope should include:

- Testing/verification of security controls, authentication techniques, access levels, etc.;
- Reviewing security monitoring processes, including network risk analysis and vulnerability assessments;
- Verifying operating controls, including balancing and separation of duties; and

- Validating the accuracy of key MIS and risk management reports.

Objective 3: Determine the quality of the institution's risk management over outsourced technology services.

1. Assess the adequacy of management's due diligence activities prior to vendor selection. Consider whether:

- Strategic and business plans are consistent with outsourcing activity, and
- Vendor information was gathered and analyzed prior to signing the contract, and the analysis considered the following:

  Vendor reputation;

  Financial condition;

  Costs for development, maintenance, and support;

  Internal controls and recovery processes; and

  Ability to provide required monitoring reports.

2. Determine whether the institution has reviewed vendor contracts to ensure that the responsibilities of each party are appropriately identified. Consider the following provisions if applicable:

- Description of the work performed or service provided;
- Basis for costs, description of additional fees, and details on how prices may change over the term of the contract;
- Implementation of an appropriate information security program;
- Audit rights and responsibilities;
- Contingency plans for service recovery;
- Data backup and protection provisions;
- Responsibilities for data security and confidentiality and language complying with the GLBA 501(b) guidelines regarding security programs;
- Hardware and software upgrades;
- Availability of vendor's financial information;

- Training and problem resolution;
- Reasonable penalty and cancellation provisions;
- Prohibition of contract assignment;
- Limitations over subcontracting (i.e., prohibition or notification prior to engaging a subcontractor for data processing, software development, or ancillary services supporting the contracted service to the institution);
- Termination rights without excessive fees, including the return of data in a machine-readable format in a timely manner;
- Financial institution ownership of the data;
- Covenants dealing with the choice of law (United States or foreign nation); and
- Rights of federal regulators to examine the services, including processing and support conducted from a foreign nation.

3. Assess the adequacy of ongoing vendor oversight. Consider whether the institution's oversight efforts include:

- Designation of personnel accountable for monitoring activities and services;
- Control over remote vendor access (e.g., dial-in, dedicated line, Internet);
- Review of service provider's financial condition;
- Periodic reviews of business continuity plans, including compatibility with those of the institution;
- Review of service provider audits (e.g., third-party reviews) and regulatory examination reports; and
- Review and monitoring of performance reports for services provided.

INFORMATION SECURITY PROCESS

Objective 4: Determine if the institution's information security program sufficiently addresses e-banking risks.

1. Determine whether the institution's written security program for customer information required by GLBA guidelines includes e-banking products and services.

2. Discuss the institution's e-banking environment with management as applicable. Based on this discussion, evaluate whether the examination scope should be expanded to include selected Tier II procedures from the IT Handbook's "Information Security Booklet." Consider discussing the following topics:

- Current knowledge of attackers and attack techniques;
- Existence of up-to-date equipment and software inventories;
- Rapid response capability for newly discovered vulnerabilities;
- Network access controls over external connections;
- Hardening of systems;
- Malicious code prevention;
- Rapid intrusion detection and response procedures;
- Physical security of computing devices;
- User enrollment, change, and termination procedures;
- Authorized use policy;
- Personnel training;
- Independent testing; and
- Service provider oversight.

3. Determine whether the security program includes monitoring of systems and transactions and whether exceptions are analyzed to identify and correct noncompliance with security policies as appropriate. Consider whether the institution adequately monitors the following:

- Systems capacity and utilization;
- The frequency and duration of service interruptions;
- The volume and type of customer complaints, including time to resolution;
- Transaction volumes by type, number, and dollar amount;
- Security exceptions;
- Unauthorized penetrations of e-banking system or network, both actual and attempted (e.g., firewall and intrusion detection system logs); and
- E-banking losses due to fraud or errors.

4. Determine the adequacy of the institution's authentication methods and need for multi-factor authentication relative to the sensitivity of systems or transactions. Consider the following processes:

- Account access
- Intrabank funds transfer
- Account maintenance
- Electronic bill payment
- Corporate cash management
- Other third-party payments or asset transfers

5. If the institution uses passwords for customer authentication, determine whether password administration guidelines adequately address the following:

- Selection of password length and composition considering ease of remembering, vulnerability to compromise, sensitivity of system or information protected, and use as single- or multi-factor authentication;
- Restrictions on the use of automatic log-on features;
- User lockout after a number of failed log-on attempts - industry practice is generally no more than 3 to 5 incorrect attempts;
- Password expiration for sensitive internal or high-value systems;
- Users' ability to select and/or change their passwords;
- Passwords disabled after a prolonged period of inactivity;
- Secure process for password generation and distribution;
- Termination of customer connections after a specified interval of inactivity - industry practice is generally not more than 10 to 20 minutes;
- Procedures for resetting passwords, including forced change at next log-on after reset;
- Review of password exception reports;
- Secure access controls over password databases, including encryption of stored passwords;
- Password guidance to customers and employees regarding prudent password selection and the importance of protecting password confidentiality; and
- Avoidance of commonly available information (i.e., name, social security number) as

user IDs.

6. Evaluate access control associated with employee's administrative access to ensure:

- Administrative access is assigned only to unique, employee-specific IDs;
- Account creation, deletion, and maintenance activity is monitored; and
- Access to funds-transfer capabilities is under dual control and consistent with controls over payment transmission channel (e.g., ACH, wire transfer, Fedline).

7. Evaluate the appropriateness of incident response plans. Consider whether the plans include:

- A response process that assures prompt notification of senior management and the board as dictated by the probable severity of damage and potential monetary loss related to adverse events;
- Adequate outreach strategies to inform the media and customers of the event and any corrective measures;
- Consideration of legal liability issues as part of the response process, including notifications of customers specifically or potentially affected; and
- Information-sharing procedures to bring security breaches to the attention of appropriate management and external entities (e.g., regulatory agencies, Suspicious Activity Reports, information-sharing groups, law enforcement, etc.).

8. Assess whether the information security program includes independent security testing as appropriate for the type and complexity of e-banking activity. Tests should include, as warranted:

- Independent audits
- Vulnerability assessments
- Penetration testing

Objective 5: Determine if the institution has implemented appropriate administrative controls to ensure the availability and integrity of processes supporting e-banking services.

1. Determine whether employee authorization levels and access privileges are commensurate with their assigned duties and reinforce segregation of duties.

2. Determine whether controls for e-banking applications include:

- Appropriate balancing and reconciling controls for e-banking activity;
- Protection of critical data or information from tampering during transmission and from viewing by unauthorized parties (e.g., encryption);
- Automated validation techniques such as check digits or hash totals to detect tampering with message content during transmission;
- Independent control totals for transactions exchanged between e-banking applications and legacy systems; and
- Ongoing review for suspicious transactions such as large-dollar transactions, high transaction volume, or unusual account activity

3. Determine whether audit trails for e-banking activities are sufficient to identify the source of transactions. Consider whether audit trails can identify the source of the following:

- On-line instructions to open, modify, or close a customer's account;
- Any transaction with financial consequences;
- Overrides or approvals to exceed established limits; and
- Any activity granting, changing, or revoking systems access rights or privileges (e.g., revoked after three unsuccessful attempts).

4. Evaluate the physical security over e-banking equipment, media, and communication lines.

5. Determine whether business continuity plans appropriately address the business impact of e-banking products and services. Consider whether the plans include the following:

- Regular review and update of e-banking contingency plans;
- Specific staff responsible for initiating and managing e-banking recovery plans;

- Adequate analysis and mitigation of any single points of failure for critical networks;
- Strategies to recover hardware, software, communication links, and data files; and
- Regular testing of back-up agreements with external vendors or critical suppliers.

LEGAL AND COMPLIANCE ISSUES

Objective 6: Assess the institution's understanding and management of legal and compliance issues associated with e-banking activities.

1. Determine how the institution stays informed on legal and regulatory developments associated with e-banking and thus ensures e-banking activities comply with appropriate consumer compliance regulations. Consider:

- Existence of a process for tracking current litigation and regulations that could affect the institution's e-banking activities;
- Assignment of personnel responsible for monitoring e-banking legislation and the requirements of or changes to compliance regulations; and
- Inclusion of e-banking activity and website content in the institution's compliance management program.

2. Review the website content for inclusion of federal deposit insurance logos if insured depository services are offered (12 CFR 328 or 12 CFR 740).

3. Review the website content for inclusion of the following information which institutions should consider to avoid customer confusion and communicate customer responsibilities:

- Disclosure of corporate identity and location of head and branch offices for financial institutions using a trade name;
- Disclosure of applicable regulatory information, such as the identity of the institution's primary regulator or information on how to contact or file a complaint with the regulator;
- Conspicuous notices of the inapplicability of FDIC/NCUA insurance to, the potential risks associated with, and the actual product provider of, the specific investment and insurance products offered;

- Security policies and customer usage responsibilities (including security disclosures and Internet banking agreements);
- On-line funds transfer agreements for bill payment or cash management users; and
- Disclosure of privacy policy - financial institutions are encouraged, but not required, to disclose their privacy policies on their websites - to include:

  "Conspicuous" disclosure of the privacy policy on the website in a manner that complies with the privacy regulation and

  Information on how to "opt out" of sharing (if the institution shares information with third parties).

4. If the financial institution electronically delivers consumer disclosures that are required to be provided in writing, assess the institution's compliance with the E-Sign Act. Review to determine whether:

- The disclosures:

  - Are clear and conspicuous;

  - Inform the consumer of any right or option to receive the record in paper or non-electronic form;

  - Inform the consumer of the right to withdraw consent, including any conditions, consequences, or fees associated with such action;

  - Inform consumers of the hardware and software needed to access and retain the disclosure for their records; and

  - Indicate whether the consent applies to only a particular transaction or to identified categories of records.
- The procedures the consumer uses to affirmatively consent to electronic delivery reasonably demonstrate the consumer's ability to access/view disclosures.

5. Determine whether e-banking support services are in place to facilitate compliance efforts, including:

- Effective customer support by the help desk, addressing:

  - Complaint levels and resolution statistics,

  - Performance relative to customer service level expectations, and

  - Review of complaints/problems for patterns or trends indicative of processing deficiencies or security weaknesses.

- Appropriate processes for authenticating and maintaining electronic signatures (E-Sign Act).

6. As applicable, determine whether the financial institution has considered the applicability of various laws and regulations to its e-banking activities:

- Monitoring of potential money-laundering activities associated with e-banking required by the Bank Secrecy Act (31 CFR 103.18);
- Filing of Suspicious Activity Reports for unusual or unauthorized e-banking activity or computer security intrusions requirements (regulation cites vary by agency);
- Screening of on-line applications and activity for entities/countries prohibited by the Office of Foreign Asset Control (31 CFR 500 et. seq.); and
- Authenticating new e-banking customers using identification techniques consistent with the requirements of Bank Secrecy Act (31 CFR 103) and the USA PATRIOT Act [12 CFR 21 (OCC), 12 CFR 208 and 211 (Board), 12 CFR 326 (FDIC), 12 CFR 563 (OTS), and 12 CFR 748 (NCUA)].

7. If overview of e-banking compliance identifies weaknesses in the institution's consideration and oversight of compliance issues, consider expanding coverage to include more detailed review using agency-specific compliance examination procedures.

EXAMINATION CONCLUSIONS

Objective 7: Develop conclusions, communicate findings, and initiate corrective action on violations and other examination findings.

1. Assess the potential impact of the examination conclusions on the institution's CAMELS and Uniform Rating System for Information Technology (URSIT) ratings.

2. As applicable to your agency, identify risk areas where the institution's risk management processes are insufficient to mitigate the level of increased risks attributed to e-banking activities. Consider:

- Transaction/operations risk
- Credit risk

- Liquidity risk
- Interest rate and price/market risk
- Compliance/legal risk
- Strategic risk
- Reputation risk

3. Prepare a summary memorandum detailing the results of the e-banking examination. Consider:

- Deficiencies noted and recommended corrective action regarding deficient policies, procedures, practices, or other concerns;
- Appropriateness of strategic and business plans;
- Adequacy and adherence to policies;
- Adequacy of security controls and risk management systems;
- Compliance with applicable laws and regulations;
- Adequacy of internal controls;
- Adequacy of audit coverage and independent security testing;
- Other matters of significance; and
- Recommendations for future examination coverage (including need for additional specialized expertise).

4. Discuss examination findings and conclusions with the examiner-in-charge. As appropriate, prepare draft report comments that address examination findings indicative of:

- Significant control weaknesses or risks (note the root cause of the deficiency, consequence of inaction or benefit of action, management corrective action, the time frame for correction, and the person responsible for corrective action);
- Deviations from safety and soundness principles that may result in financial or operational deterioration if not addressed; or
- Substantive noncompliance with laws or regulations.

5. In coordination with the examiner-in-charge, discuss findings with institution

management including, as applicable, conclusions regarding applicable ratings and risks. If necessary, obtain commitments for corrective action.

6. Revise draft e-banking comments to reflect discussions with management and finalize comments for inclusion in the report of examination.

7. As applicable, according to your agency's requirements/instructions, include written comments specifically stating what the regulator should do in the future to effectively supervise e-banking in this institution. Include supervisory objectives, time frames, staffing, and workdays required.

8. Update the agency's information systems and applicable report of examination schedules or tables as applicable.

E-Banking Request Letter Items

Objective 1 - Determine the scope for the examination of the institution's e-banking activities consistent with the nature and complexity of the institution's operations.

- An organization chart of e-banking personnel including the name, title, and phone number of the e-banking examination contact.
- A list of URLs for all financial institution-affiliated websites.
- A list all e-banking platforms utilized and network diagrams including servers, routers, firewalls, and supporting system components.
- A list of all e-banking related products and services including transaction volume data on each if it is available.
- A description of any changes in e-banking activities or future e-banking plans since the last exam.
- Diagrams illustrating the e-banking transaction workflow.
- Copies of recent monitoring reports that illustrate trends and experiences with intrusion attempts, successful intrusions, fraud losses, service disruptions, customer complaint volumes, and complaint resolution statistics.
- Copies of findings from, and management/board responses to, the following:

  - Internal and external audit reports (including third-party reviews on service providers and testing of the information security program),

  - Annual tests of the written information security program as required by GLBA,

- Vulnerability assessments,

- Penetration tests, and

- Other independent security tests or e-banking risk reviews

Objective 2 - Determine the adequacy of board and management oversight of e-banking activities with respect to strategy, planning, management reporting, and audit.

- Internal or external audit schedules, audit scope, and background/training information on individuals conducting e-banking audits.
- Descriptions of e-banking-related training provided to employees including date, attendees, and topics.
- Strategic plans or feasibility studies related to e-banking.
- Insurance policies covering e-banking activities such as blanket bond, errors and omissions, and any riders relating to e-banking.
- Copies of recent management and board reports that measure or analyze e-banking performance both strategically and technically, such as percentage of customers using e-banking channels or system capacity to maintain current and planned level of transactional activity.

Objective 3 - Determine the quality of the institution's risk management over outsourced technology services.

- Policies and procedures related to vendor management
- A list of all third-party providers, contractors, or support vendors, including the name, services provided, address, and phone number for each.
- Documentation supporting initial or ongoing due diligence of the above vendors including financial condition, service level performance, security reporting, audit reports, security assessments, and disaster recovery tests as appropriate.
- Vendor contracts (make available upon request).

Objective 4 - Determine if the institution has appropriately modified its information security program to incorporate e-banking risks.

- Findings from security risk assessments pertaining to e-banking activities.

- Information security policies and procedures associated with e-banking systems, products, or services, including policies associated with customer authentication, employee e-mail usage, and Internet usage.
- A list or report of authorized users and access levels for e-banking platforms, including officers, employees, system vendors, customers, and other users.
- Samples of e-banking-related security reports reviewed by IT management, senior management, or the board including suspicious activity, unauthorized access attempts, outstanding vulnerabilities, fraud or security event reports, etc.
- Documentation related to any successful e-banking intrusion or fraud attempt.

If e-banking is hosted internally, provide the following additional information:

- A list of security software tools employed by the institution including product name, vendor name, and version number for filtering routers, firewalls, network-based intrusion detection software (IDS), host-based IDS, and event correlation analysis software (illustrate placement on network diagram);
- Policies related to identification and patching of new vulnerabilities; and
- Descriptions of router access control rules, firewall rules, and IDS event detection and response rules including the corresponding logs.

Objective 5 - Determine if the institution has implemented appropriate administrative controls to ensure the availability, and integrity of processes supporting e-banking services.

- E-banking policies and procedures related to account opening, customer authentication, maintenance, bill payment or e-banking transaction processing, settlement, and reconcilement.
- Business resumption plans for e-banking services.

Objective 6 - Assess the institution's understanding and management of legal and compliance issues associated with e-banking activities.

- Policies and procedures related to e-banking consumer compliance issues including website content, disclosures, BSA, financial record keeping, and the institution's trade area.
- A list of any pending lawsuits or contingent liabilities with potential losses relating to e-banking activities.

- Documentation of customer complaints related to e-banking products and services.
- Copies of, or publicly available weblinks to, privacy statements, consumer compliance disclosures, security disclosures, and e-banking agreements.

If financial institution provides cross-border e-banking products and services, provide the following additional information.

- Policies for, or a description of, permissible cross-border e-banking including types of products and services such as account opening, account access, or funds transfer, and restrictions such as geographic location, citizenship, etc.
- Policies for, or a description of, the institution's due diligence process for accepting cross-border business.

Appendix B: Glossary

Digital certificate - The electronic equivalent of an ID card that authenticates the originator of a digital signature.

Direct data feed - A process used by information aggregators to gather information directly from a website operator rather than copying it from a displayed webpage.

E-Banking - The remote delivery of new and traditional banking products and services through electronic delivery channels.

E-mail server - A computer that manages e-mail traffic.

Encryption - A data security technique used to protect information from unauthorized inspection or alteration. Information is encoded so that data appears as a meaningless string of letters and symbols during delivery or transmission. Upon receipt, the information is decoded using an encryption key.

Firewall - A hardware or software link in a network that relays only data packets clearly intended and authorized to reach the other side.

Framing - A frame is an area of a webpage that scrolls independently of the rest of the webpage. Framing generally refers to the use of a standard frame containing information (like company name and navigation bars) that remains on the screen while the user moves around the text in another frame.

Gateway server - A computer (server) that connects a private network to the private network of a servicer or other business.

Hacker - An individual who attempts to break into a computer without authorization.

Hardening - The process of securing a computer's administrative functions or inactivating those features not needed for the computer's intended business purpose.

Hash Totals - A numerical summation of one or more corresponding fields of a file that would not ordinarily be summed. Typically used to detect when changes in electronic information have occurred.

Hosting - See "Website Hosting".

Hyperlink - An item on a webpage that, when selected, transfers the user directly to another location in a hypertext document or to another webpage, perhaps on a different machine. Also simply called a "link."

Hypertext Markup Language (HTML) - A set of codes that can be inserted into text files to indicate special typefaces, inserted images, and links to other hypertext documents.

Interface - Computer programs that translate information from one system or application into a format required for use by another system or application.

Internet - The global system of interconnected computer networks that use the Internet protocol suite (TCP/IP) to link billions of devices worldwide.

Internet service provider (ISP) - A company that provides its customers with access to the Internet (e.g., AT&T, Verizon, CenturyLink).

Interoperability standards/protocols - Commonly agreed on standards that enable different computers or programs to share information. Example: HTTP (Hypertext Transfer Protocol) is a standard method of publishing information as hypertext in HTML format on the Internet.

Kiosk - A publicly accessible computer terminal that permits customers to directly communicate with the financial institution via a network.

Legacy systems - A term commonly used to refer to existing computers systems and applications with which new systems or applications must exchange information.

Lockout - The action of temporarily revoking network or application access privileges, normally due to repeated unsuccessful logon attempts.

Mnemonic - A symbol or expression that can help someone remember something. For example, the phrase "Hello! My name is Bill. I'm 9 years old." might help an individual remember a secure 10-character password of "H!MniBI9yo."

Network administrator - The individual responsible for the installation, management, and control of a network.

Network diagram - A description of any kind of locality in terms of its physical layout. In the context of communication networks, a topology describes pictorially the configuration or arrangement of a network, including its nodes and connecting communication lines.

Passwords - A secret sequence of characters that is used as a means of authentication.

Patching - Software code that replaces or updates other code. Frequently patches are used to correct security flaws.

Penetration test - The process of using approved, qualified personnel to conduct real-world attacks against a system to identify and correct security weaknesses before they are discovered and exploited by others.

Personal digital assistant (PDA) - A pocket-sized, special-purpose personal computer that lacks a conventional keyboard.

Phishing - A digital form of social engineering that uses authentic-looking—but bogus—e-mail to request information from users or direct them to fake websites that request information.

Pop-up box - A dialog box that automatically appears when a person accesses a webpage.

Private key infrastructure (PKI) - The use of public key cryptography in which each customer has a key pair (e.g., a unique electronic value called a public key and a mathematically-related private key). The private key is used to encrypt (sign) a message that can only be decrypted by the cor-responding public key or to decrypt a message previously encrypted with the public key. The public key is used to decrypt a message previously encrypted (signed) using an individual's private key or to encrypt a message so that it can only be decrypted (read) using the intended recipient's private key.

Proxy server - An Internet server that controls client computers' access to the Internet. Using a proxy server, a company can stop employees from accessing undesirable websites, improve performance by storing webpages locally, and hide the internal network's identity so monitoring is difficult for external users.

Public key - See "PKI".

Repudiation - The denial by one of the parties to a transaction of participation in all or part of that transaction or of the content of the communication.

Router - A hardware device that connects two or more networks and routes incoming data packets to the appropriate network.

Script - A file containing active content; for example, commands or instructions to be executed by the computer.

Secure Socket Layer (SSL) - A protocol that is used to transmit private documents through the Internet.

Server - A computer or other device that manages a network service. An example is a print server, which is a device that manages network printing.

Smart cards - A card with an embedded computer chip on which information can be stored and processed.

Sreen scraping - A process used by information aggregators to gather information from a customer's website, whereby the aggregator accesses the target site by logging in as the customer, electronically reads and copies selected information from the displayed webpage(s), then redisplays the information on the aggregator's site. The process is analogous to "scraping" the information off the computer screen.

Suspicious activity report (SAR) - Reports required to be filed by the Bank Secrecy Act when a financial institution identifies or suspects fraudulent activity.

Token - A small device with an embedded computer chip that can be used to store and transmit electronic information. A soft token is a software-based token.

Topology - See "Network diagram".

Uniform Resource Locator (URL) - Abbreviation for "Uniform (or Universal) Resource Locator." A way of specifying the location of publicly available information on the Internet, in the form: protocol://machine:port number/filename. Often the port number and/or filename are unnecessary.

Virtual Mall - An Internet website offering products and services from multiple vendors or suppliers.

Virtual private network (VPN) - A computer network that uses public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organization's network.

Virus - Malicious code that replicates itself within a computer.

Weblinking - The use of hyperlinks to direct users to webpages of other entities.

Website - A webpage or set of webpages designed, presented, and linked together to form a logical information resource and/or transaction initiation function.

Website hosting - The service of providing ongoing support and monitoring of an

Internet-addressable computer that stores webpages and processes transactions initiated over the Internet.

Wireless application protocol (WAP) - A data transmission standard to deliver wireless markup language (WML) content.

Wireless gateway server - A computer (server) that transmits messages between a computer network and a cellular telephone or other wireless access device.

Wireless phone - See "Cellular Telephone".

Worm - A self-replicating malware computer program. It uses a computer network to send copies of itself to other nodes (computers on the network) and it may do so without any user intervention. This is primarily because of security vulnerabilities on the target computers.

Appendix C: Laws, Regulations, and Guidance

Laws

- 12 USC 1861-1867(c): Bank Service Company Act (N/A)
- 15 USC 6801 and 6805(b): Gramm-Leach-Bliley Act (GLBA) (N/A)
- 18 USC 1030: Fraud and Related Activity in Connection with Computers (N/A)
- Pub. L. No. 106-229: Electronic Signatures in Global and National Commerce Act (E-Sign Act) (N/A)
- Pub. L. No. 107-56: USA PATRIOT Act (N/A)

Federal Reserve Board

- 12 CFR 208.62: Suspicious Activity Reports (N/A)
- 12 CFR Part 208: Interagency Guidelines Establishing Standards for Safeguarding Customer Information, Appendix D-2 (State Member Banks) (N/A)
- 12 CFR 211.5: Interagency Guidelines Establishing Standards for Safeguarding Customer Information (Edge or agreement corporation) (N/A)
- 12 CFR 211.24: Interagency Guidelines Establishing Standards for Safeguarding Customer Information (uninsured state-licensed branch or agency of a foreign bank) (N/A)
- 12 CFR Part 225 Appendix F: Interagency Guidelines Establishing Standards for Safeguarding Customer Information (bank holding companies and their non-bank subsidiaries or affiliates) (N/A)
- SR Letter 01-20: FFIEC Guidance on Authentication (August 15, 2001)
- SR Letter 01-15: Standards for Safeguarding Customer Information (May 31, 2001)
- SR Letter 01-11: Identity Theft and Pretext Calling (April 26, 2001)
- SR Letter 00-17: Guidance on the Risk Management of Outsourced Technology Services (November 30, 2001)
- SR Letter 00-05: Lessons Learned from the Year 2000 Project (March 31, 2000)
- SR Letter 00-04: Outsourcing of Information and Transaction Processing (February 29, 2000)
- SR Letter 00-03: Information Technology Examination Frequency (February 29,

2000)

- SR Letter 99-08: Uniform Rating System for Information Technology (March 31, 1999)
- SR Letter 98-14: Interagency Policy Statement on Branch Names (June 3, 1998)
- SR Letter 98-09: Assessment of Information Technology in the Risk-Focused Frameworks for the Supervision of Community Banks and Large Complex Banking Organizations (April 20, 1998)
- SR Letter 97-32: Sound Practices Guidance for Information Security for Networks (December 4, 1997)
- SR Letter 97-28: Guidance Concerning the Reporting of Computer-Related Crimes by Financial Institutions (November 6, 1997)

Federal Deposit Insurance Corporation

- 12 CFR Part 328: FDIC Advertisement of Membership (N/A)
- 12 CFR Part 353: Suspicious Activity Reports (N/A)
- 12 CFR Part 364 Appendix B: Interagency Guidelines Establishing Standards for Safeguarding Customer Information (N/A)
- FIL-30-2003: Weblinking (April 23, 2003)
- FIL-8-2002: Wireless Networks And Customer Access (February 1, 2002)
- FIL-69-2001: Authentication in an Electronic Banking Environment (August 24, 2001)
- FIL-50-2001: Bank Technology Bulletin on Outsourcing (June 4, 2001)
- FIL-68-2001: 501(b) Examination Guidance (August 24, 2001)
- FIL-33-2001: Electronic Funds Transfers (April 20, 2001)
- FIL-25-2001: Electronic Funds Transfers (March 23, 2001)
- FIL-22-2001: Security Standards for Customer Information (March 14, 2001)
- FIL-81-2000: Risk Management of Technology Outsourcing (November 29, 2000)
- FIL-77-2000: Bank Technology Bulletin: Protecting Internet Domain Names (November 9, 2000)
- FIL-72-2000: Electronic Signatures in Global and National Commerce Act (November 2, 2000)
- FIL-67-2000: Security Monitoring of Computer Networks (October 3, 2000)
- FIL-63-2000: Online Banking (September 21, 2000)

- FIL-68-99: Risk Assessment Tools And Practices For Information System Security (July 7, 1999)
- FIL-49-99: Bank Service Company Act (June 3, 1999)
- FIL-98-98: Pretext Phone Calling (September 2, 1998)
- FIL-86-98: Electronic Commerce and Consumer Privacy (August 17, 1998)
- FIL-79-98: Electronic Financial Services and Consumer Compliance (July 16, 1998)
- FIL-46-98: Guidance on the Use of Trade Names (May 1, 1998)
- FIL-131-97: Security Risks Associated with the Internet (December 18, 1997)
- FIL-124-97: Suspicious Activity Reporting (December 5, 1997)
- FIL-14-97: Electronic Banking Examination Procedures (February 26, 1997)
- FIL-59-96: Stored Value Cards and Other Electronic Payment Systems (August 6, 1996)

National Credit Union Administration

- 12 CFR Part 721: Incidental Powers (N/A)
- 12 CFR Part 748: Security Program, Report of Crime and Catastrophic Act and Bank Secrecy Act Compliance (N/A)
- 12 CFR Part 716: Privacy of Consumer Financial Information & Appendix (N/A)
- 12 CFR Part 741: Requirements for Insurance (N/A)
- 12 CFR Part 740: Advertising (N/A)
- NCUA Letter to Credit Unions 03-CU-08: Weblinking: Identifying Risks & Risk Management Techniques (April 2003)
- NCUA Letter to Credit Unions 02-CU-17: E-Commerce Guide for Credit Unions (December 2002)
- NCUA Letter to Credit Unions 02-CU-16: Protection of Credit Union Internet Addresses (December 2002)
- NCUA Letter to Federal Credit Unions 02-FCU-11: Tips to Safely Conduct Financial Transactions Over the Internet-An NCUA Brochure for Credit Union Members (July 2002)
- NCUA Letter to Credit Unions 02-CU-13: Vendor Information Systems & Technology Reviews-Summary Results (July 2002)
- NCUA Letter to Credit Unions 02-CU-08: Account Aggregation Services (April 2002)

- NCUA Letter to Federal Credit Unions 02-FCU-04: Weblinking Relationships (March 2002)
- NCUA Letter to Credit Unions 01-CU-20: Due Diligence Over Third-Party Service Providers (November 2001)
- NCUA Letter to Credit Unions 01-CU-12: E-Commerce Insurance Considerations (October 2001)
- NCUA Letter to Credit Unions 01-CU-09: Identity Theft and Pretext Calling (September 2001)
- NCUA Letter to Credit Unions 01-CU-11: Electronic Data Security Overview (August 2001)
- Authentication in an Electronic Banking Environment, NCUA Letter to Credit Unions 01-CU-10 (August 2001)
- NCUA Regulatory Alert 01-RA-03: Electronic Signatures in Global and National Commerce Act (E-Sign Act) (March 2001)
- NCUA Letter to Credit Unions 01-CU-02: Privacy of Consumer Financial Information (February 2001)
- NCUA Letter to Credit Unions 00-CU-11: Risk Management of Outsourced Technology Services (with Enclosure) (December 2000)
- NCUA Letter to Credit Unions 00-CU-07: NCUA's Information Systems & Technology Examination Program (October 2000)
- NCUA Letter to Credit Unions 00-CU-04: Suspicious Activity Reporting (see section on "Computer Intrusion") (June 2000)
- NCUA Letter to Credit Unions 00-CU-02: Identity Theft Prevention (May 2000)
- NCUA Regulatory Alert 99-RA-3: Pretext Phone Calling by Account Information Brokers (February 1999)
- NCUA Regulatory Alert 9--RA-4: Interagency Guidance on Electronic Financial Services and Consumer Compliance (July 1998)
- NCUA Letter to Credit Unions 97-CU-5: Interagency Statement on Retail On-Line PC Banking, (April 1997)
- NCUA Letter to Credit Unions 97-CU-1: Automated Response System Controls (January 1997)

Office of the Comptroller of the Currency

- 12 CFR 7.1002: National Banks Acting as Finder (N/A)
- 12 CFR Part 7, Subpart E: Electronic Activities (N/A)

- 12 CFR Part 21, Subpart B: Reports of Suspicious Activities (N/A)
- 12 CFR Part 30, Appendix B: Interagency Guidelines Establishing Standards for Safeguarding Customer Information (N/A)
- OCC Bulletin 2003-15: Weblinking: Interagency Guidance on Weblinking Activity (April 23, 2003)
- OCC Bulletin 2002-16: Bank Use of Foreign-Based Third-Party Service Providers (May 15, 2002)
- OCC Bulletin 2002-2: ACH Transactions Involving the Internet (January 14, 2002)
- OCC Bulletin 2001-47: Third-Party Relationships (November 1, 2001)
- OCC Advisory Letter 2001-8: Authentication in an Electronic Banking Environment (July 30, 2001)
- OCC Bulletin 2001-35: Examination Procedures to Evaluate Compliance with the Guidelines to Safeguard Customer Information (July 18, 2001)
- OCC Bulletin 2001-23: Uniform Standards for the Electronic Delivery of Disclosures; Regulations M, Z, B, E and DD (April 27, 2001)
- OCC Advisory Letter 2001-04: Identity Theft and Pretext Calling (April 30, 2001)
- OCC Alert 2001-04: Network Security Vulnerabilities (April 24, 2001)
- OCC Bulletin 2001-12: Bank-Provided Account Aggregation Services (February 28, 2001)
- Suspicious Activity Report, OCC Bulletin 2000-19 (June 2000)
- OCC Alert 2000-9: Protecting Internet Addresses of National Banks (July 19, 2000)
- OCC Bulletin 99-20: Certification Authority Systems (May 4, 1999)
- OCC Bulletin 98-22: Branch Names (May 12, 1998)
- OCC Advisory Letter 97-9: Reporting Computer-Related Crimes (November 19, 1997)

Office of Thrift Supervision

- 12 CFR Part 555: Electronic Operations (N/A)
- 12 CFR 563.180: Suspicious Activity Reports and Other Reports and Statements (N/A)
- 12 CFR Part 568: Security Procedures Under the Bank Protection Act (N/A)
- 12 CFR Part 570 Appendix B: Interagency Guidelines Establishing Standards for

Safeguarding Customer Information (N/A)

- 12 CFR Part 573: Privacy of Consumer Financial Information (N/A)
- CEO Ltr 155: Interagency Guidance: Privacy of Consumer Financial Information (February 11, 2002)
- CEO Ltr 143: Interagency Guidance on Authentication in an Electronic Banking Environment (transmits FFIEC document, Authentication in an Electronic Banking Environment) (August 9, 2001)
- CEO Ltr 139: Identity Theft and Pretext Calling (May 4, 2001)
- CEO Ltr 109: Transactional Web Sites (June 10, 1999)
- CEO Ltr 97: Policy Statement on Privacy and Accuracy of Personal Customer Information and Interagency Pretext Phone Calling Memorandum (November 3, 1998)
- CEO Ltr 86: Interagency Statement on Branch Names (June 11, 1998)
- CEO Ltr 70: Statement on On-Line Personal Computer Banking (June 23, 1997)

Appendix D: Aggregation Services

OVERVIEW

Account aggregation is a service that gathers information from many websites and presents that information in a consolidated format to the customer. The information gathered can range from publicly available information to personal account information (e.g., credit card, brokerage, and banking data). Typically, the aggregator obtains the personal account information by using customer-provided usernames and passwords to enter websites. Aggregators typically collect information through direct data feeds from the aggregation target or by "scraping" the information from the targeted webpages. The collection method used varies based on the aggregator's relationship with the operator of the target website. Emerging capabilities include offering customers the ability to initiate transactions, obtain financial advice, and use shopping services to scan the Web for products. Many experts believe institutions that provide aggregation services have the opportunity to deepen their customer relationships by leveraging their position as trusted financial intermediaries.

RISK IMPLICATIONS

Financial institutions engaged in aggregation services assume an increased level of risk and must institute compensating risk management practices.

Transaction/operations risk - The highly sensitive nature of the information collected and stored by aggregators greatly increases the risk associated with aggregation services. The aggregator's ability to protect stored customer IDs and passwords and to provide accurate and timely delivery of information from the customer's accounts is the most significant factor in assessing the level of operations risk in aggregation services.

Strategic risk - Strategic risk is the second highest exposure in aggregation services. This is due not only to the relatively unproven success of this service, but also to the fact that the applicability of legal and compliance requirements to the service have yet to be fully defined.

Reputation risk - Reputation risk is another significant consideration in aggregation services. However, in most instances it is a second-tier issue (i.e., potential damage to the institution's reputation stemming from operational or legal risk issues discussed above).

RISK MANAGEMENT

Risk management of aggregation services is based on the same concepts that apply to other financial services (i.e. risk identification, measurement, monitoring and control). Some of the unique concerns financial institutions should consider in managing aggregation risks are discussed below.

AGGREGATION SERVICE PROVIDERS

Typically, a financial institution provides an aggregation service under its brand name through a third-party service provider. That service provider serves as a prime contractor, specializing in gathering, storing, protecting, and presenting information to the customer. The third-party service provider, in turn, may outsource some of its features, such as bill payment, to other specialists. The institution or third-party service provider also may provide or outsource software that analyzes customer behavior and suggests financial products for that customer. Aggregated financial information often comes from other websites, the owners of which may not be aware that they are providing content and thus lack contracts or agreements with the aggregating institution or service provider.

Because aggregation is at an early stage of development and customer acceptance is low, institutions should consider how evolving standards and customer acceptance for aggregation services may affect e-banking strategies. Further, reliance on third-party service providers introduces strategic risks that institutions should consider. For example, some third-party service providers may be financially unstable or unable to provide reliable service. Others may develop or market services in ways that are incompatible with the institution's goals. Further, some arrangements, such as co-branding, may make it more difficult to change providers, if problems arise.

The viability of aggregation services depends heavily on meeting customer expectations, including availability, confidentiality, data integrity, and overall service quality. Moreover, as customer acceptance grows, customers are likely to expect aggregator institutions to innovate and provide additional services. Failure to meet customer expectations (whether provided by the institution or a third-party provider) can undermine customer confidence and trust. This could hinder the institution's ability to retain existing customers and to offer other e-banking products and services in the future.

TRANSACTION SECURITY

Aggregation relies on data transmission from various websites through the aggregator's website to the end-customer's Internet browser. If the integrity of the data is compromised or if the data is not current, the customer could receive erroneous or dated information, which could adversely affect customer decisions. Timely and correct information is especially important in environments where purchases, sales, and asset transfers take place.

Information security is critical because aggregators centralize the storage of usernames and passwords that provide access to other websites, as well as personally identifiable customer information from many other websites. A security breach could compromise numerous customer accounts. Because sensitive information is centralized, attackers may be more likely to target the aggregator's systems. A financial institution acting as an aggregator should carefully consider its potential liabilities and assess whether it and its third-party providers have adequate security.

Inadequate authentication measures may expose aggregator institutions to liability if these measures weaken the security of other websites. Because both the aggregator and the customer typically enter the target website using the same username and password, the target Website may not be able to identify the true system user (i.e., customer or aggregator), diminishing the effectiveness of the target's access controls and record keeping. Additionally, entry to the target website may be gained automatically at the aggregator's website, effectively bypassing some of the target website's protections against fraud and theft of authentication devices.

Aggregators that receive and facilitate transactions have the additional risk of liability for unauthorized or disputed transactions. In situations where a dispute arises after an aggregator communicates a request from the customer to another website, the aggregator may need to trace the transaction. If the aggregator does not have good audit trails that prove the customer originated the transaction and that the transaction was transmitted correctly, the aggregator or institution would be potentially liable.

DATA GATHERING

Aggregators typically collect data from target websites by one of two means: screen scraping or direct data feeds. Screen scraping involves copying information from a target webpage accessed using the customer's previously provided password and PIN. Such activity may occur without the consent or knowledge of the target website. Direct data feeds involve the cooperative exchange of information between the target website and the aggregator. Data-feed arrangements frequently reduce transaction risk by implementing technologies that are more reliable and traceable than other data-gathering techniques.

In some cases, aggregators may be blocked from gaining access to information from target websites. For example, target websites may change the location of information on a webpage or change passwords. Additionally, the target websites may have data integrity problems that they report on their webpage. This information may not be captured by the aggregator's information collection mechanisms and reported to the institution's customers. Such situations may result in failing to meet customer expectations and may result in inaccurate or incomplete information. Another challenge facing aggregators is the interpretation and accurate presentation of the data gathered from other websites. For example, aggregators may discover similarly named data elements have different definitions. An incorrect presentation of data could result in customer confusion and incorrect decisions.

LEGAL AND COMPLIANCE REQUIREMENTS

Aggregation services raise three key compliance risks issues: the application of Regulation E, asset management, and privacy.

Regulation E

In aggregating customer information, institutions should closely monitor regulatory changes in the application of Regulation E. Currently, Regulation E, which implements the Electronic Fund Transfer Act, does not specifically address the responsibilities of aggregators. The Federal Reserve Board requested comments on this issue in June 2000. A final regulation had not been issued at the time of this booklet's issuance. In the absence of guidance, institution management should be conservative when interpreting possible Regulation E compliance obligations in connection with aggregation services.

Aggregators that provide electronic fund transfer services could come within the current coverage of Regulation E in the following ways.

- If the aggregator is a financial institution and holds consumer accounts in the institution, the aggregator is covered by Regulation E when it agrees with the consumer to provide electronic fund transfer services to or from the account.
- If an aggregator institution issues a card, PIN, or other access device to the consumer and agrees to provide electronic fund transfer services with respect to accounts at other institutions it is generally covered by Regulation E. However, if the aggregator institution does not have an agreement with these other institutions concerning the electronic fund transfer services, a special set of rules under Regulation E for "service providers" applies.

Institutions and aggregation service providers should also consider the possibility that providing customers with an automatic log-on feature to conduct electronic fund transfers on other entities' websites could trigger the application of Regulation E if such automatic log-on features could be considered, in essence, an access device for electronic fund transfer services.

Asset Management

Asset management encompasses a broad range of activities, such as trust and fiduciary services, retail brokerage, and financial planning, where investment advice is provided for a fee or commission. In particular, institutions aggregating clients' account information should ensure compliance with the Bank Secrecy Act. Depending on the nature of the services provided in connection with aggregation of account information, financial institutions should also comply with the Employee Retirement Income Security Act of 1974 (ERISA), and other applicable laws, regulations, and policies. Banks should also comply with applicable fiduciary standards imposed pursuant to 12 CFR Part 9 and savings associations should also comply with 12 CFR part 550.

In addition to aggregating account information, aggregator institutions may provide links to affiliated and unaffiliated third-party websites that allow consumers to buy securities and insurance products directly. In these instances, institutions should clearly distinguish on their websites between products and services that are offered by the institution and those offered by third parties. In general, the institution should use clear and conspicuous language to explain their role and responsibility for products and services offered on any third-party webpages. For institution webpages that provide links to third-party pages that enable institution customers to open accounts or initiate transactions for non-deposit investment products, the disclosures also should alert customers to risks associated with those products (e.g., by stating that the products are not insured by the FDIC, are not a deposit, and may lose value).

Privacy

Institutions that provide aggregation services should be aware of various legal provisions protecting the confidentiality of consumer information that affect aggregation activities. Institutions are strongly advised to evaluate the privacy provisions of GLBA and requirements of the Fair Credit Reporting Act (FCRA) regarding the disclosure of consumer information received in connection with providing aggregation services. In particular, a financial institution that provides aggregation services should ensure that its privacy policy required by GLBA accurately reflects the categories of information that it collects and discloses in its aggregator role, which may differ from the types of information that the institution collects and discloses with respect to customers of its own banking products or services. Institutions also should be aware that a financial institution may freely disclose to other parties its own transaction or experience information that bears on consumers' creditworthiness, personal characteristics, or mode of living. However, the sharing of information-to affiliates or other unrelated third parties-that does not relate to a financial institution's own transactions and experiences may trigger the requirements of FCRA.

It is important to note that compliance with one statute will not guarantee compliance with the other.

RECORD KEEPING

If aggregation services include the initiation of transactions, institution management should assure aggregation processes are sufficiently robust to address issues relating to the validity of transactions, such as attribution and non-repudiation. Those processes go beyond security measures and encompass coordination of record keeping with other websites. That coordination should be sufficient to enable the tracing of a transaction from the customer through the institution to the other websites, with reasonable controls to protect against unauthorized changes to the transaction. Good records can improve a financial institution's position in the event of disputes. Record keeping requirements should be based upon the level of activity and risk.

CONTRACTS

Appropriate contracting can mitigate strategic, reputation, transaction, and compliance risks. Management should seek to control and manage these risks by structuring arrangements between the institution and the involved parties. Standardized contracts and the development and use of industry standards can facilitate those arrangements.

Customer Agreements

Contracting will primarily involve the institution, the institution's customer, and the aggregation technology provider. Customer agreements should specify the scope of the aggregating institution's authority to use the customers' passwords and other authenticators on their behalf. Moreover, customers should be advised of the degree of responsibility the institution assumes for the timeliness or accuracy of the information obtained from other websites.

The customer contract should provide the basis for realistic expectations about such matters as data timeliness and completeness, support, and service levels. For instance, transaction risks relating to data definitions and timing can be controlled by clearly disclosing when the aggregated information was obtained from the other websites and any material changes in the definition of data elements. Institutions should consider how best to direct customers to those customer service areas, whether at the institution, technology provider, or operator of another website that can most directly and effectively help resolve customer issues. Institutions should also be aware that the websites where information is aggregated might post disclosures that belong with the aggregated information. Management should consider whether and how to notify their customers of those disclosures.

Vendor Contracts

The institution's contracts with technology providers should ensure the provided activities conform to applicable legal and policy standards, and should acknowledge the institution's regulator's authority to examine and regulate the provided activities authorized by 12 USC 1867(c) for banks and 12 USC 1464(d)(7) for savings associations. The contract should clearly disclose and authorize the roles and responsibilities of the institution and the technology provider. Contracts also should cover security requirements and reporting, performance reporting, data usage restrictions, data ownership, indemnification arrangements, data retention policies, business continuation arrangements, and submission of financial statements.

Contracts with Other Websites

To the extent that agreements with other websites are practical, those agreements should address:

- System security applicable to the acquired data and authentication information;
- Use of customer information;
- Timing and method of data access;
- Methods for verifying the aggregator's authority to access data on behalf of the consumer (including the authentication and authorization procedures used to verify the identity of account holders);
- Need for transaction logs of specific consumer instructions for the aggregator;
- Responsibility for the timeliness and accuracy of information to be provided; and
- Responsibility for delivery of disclosures and consumer notifications.

Appendix E: Wireless Banking

OVERVIEW

Wireless banking occurs when a customer accesses a financial institution's networks through cellular phones, pagers, and personal digital assistants (or similar devices) via telecommunication companies' wireless networks. While wireless services can extend the reach and enhance the convenience of an institution's banking products and services, wireless communications currently have certain limitations that tend to increase the risks associated with this delivery channel.

RISK IMPLICATIONS

Wireless banking services can significantly increase a financial institution's level of transaction/operations and strategic risks.

Transaction/Operations risk - Wireless services create a heightened level of potential operations risk due to limitations in wireless technology. Security solutions that work in wired networks must be modified for application in a wireless environment. The transfer of information from a wired to a wireless environment can create additional risks to the integrity and confidentiality of the information exchanged.

Strategic risk - Financial institutions considering wireless services should carefully evaluate the significant strategic risks posed by this service delivery channel. Standards for wireless communication are still evolving, creating considerable uncertainty regarding the scalability of existing wireless products. Financial institutions should exercise extra diligence in preparing and evaluating the cost-effectiveness of investments in wireless technology or in decisions committing the institution to a particular wireless solution, vendor or third-party service provider.

RISK MANAGEMENT

Risk management of wireless-based technology solutions, although similar to other electronic delivery channels, may involve unique challenges created by the current state of wireless services and wireless devices. Some of these special considerations are discussed below.

MESSAGE ENCRYPTION

Encryption of wireless banking activities is essential because wireless communications can be recorded and replayed to obtain information. Encryption of wireless communications can occur in the banking application, as part of the data transmission process, or both.

Transactions encrypted in the banking application (e.g., bank-developed for a PDA) remain encrypted until decrypted at the institution. This level of encryption is unaffected by the data transmission encryption process. However, banking application-level encryption typically requires customers to load the banking application and its encryption/decryption protocols on their wireless device. Since not all wireless devices provide application-loading capabilities, requiring application level encryption may limit the number of customers who can use wireless services.

Wireless encryption that occurs as part of the data transmission process is based upon the device's operating system. A key risk-management control point in wireless banking occurs at the wireless gateway-server where a transaction is converted from a wireless standard to a secure socket layer (SSL) encryption standard and vice versa. Wireless network security reviews should focus on how institutions establish, maintain, and test the security of systems throughout the transmission process, from the wireless device to the institutions' systems and back again. For example, a known wireless security vulnerability exists when the Wireless Application Protocol (WAP) transmission encryption process is used. WAP transmissions deliver content to the wireless gateway-server where the data is decrypted from WAP encryption and re-encrypted for Internet delivery. This is often called the "gap-in-WAP" (e.g., wireless transport layer security (TLS) to Internet-based TLS). This brief instant of decryption increases risk and becomes an important control point, as the transaction may be viewable in plain text (unless encryption also occurred in the application layer). The WAP Forum, a group that oversees WAP protocols and standards, is discussing ways to reduce or eliminate the gap-in-WAP security risk.

Institutions must ensure effective controls are in place to reduce security vulnerabilities and protect data being transmitted and stored. Under the GLBA guidelines, institutions considering implementing wireless services are required to ensure that their information security program adequately safeguards customer information.

PASSWORD SECURITY

Wireless banking increases the potential for unauthorized use due to the limited availability of authentication controls on wireless devices and higher likelihood that the device may be lost or stolen. Authentication solutions for wireless devices are currently limited to username and password combinations that may be entered and stored in clear text view (i.e., not viewed as asterisks "****"). This creates the risk that authentication credentials can be easily observed or recalled from a device's stored memory for unauthorized use.

Cellular phones also have more challenging methods to enter alphanumeric passwords. Customers need to depress telephone keys multiple times to have the right character displayed. This process is complicated if a phone does asterisk password entries, as the user may not be certain that the correct password is entered. This challenge may result in users selecting passwords and personal identification numbers that are simple to enter and easy to guess.

STANDARDS AND INTEROPERABILITY

The wireless device manufacturers and content and application providers are working on common standards so that device and operating systems function seamlessly. Standards can play an integral role in providing a uniform entry point to legacy transaction systems. A standard interface would allow institutions to add and configure interfaces, such as wireless delivery, without having to modify or re-write core systems. Interoperability is a critical component of mobile wireless because there are multiple device formats and communication standards that can vary the users' experience.

WIRELESS VENDORS

Institutions typically rely on third-party providers to develop and deliver wireless banking applications. Reliance on third parties is often necessary to gain wireless expertise and to keep up with technology advancements and evolving standards. Third-party providers of wireless banking applications include existing Internet banking application providers and as well as new service providers specializing in wireless communications. These companies facilitate the transmission of data from the wireless device to the Internet banking application. Outsourced services may also include managing product and service delivery to multiple types of devices using multiple communication standards. Institutions that rely on service providers to provide wireless delivery systems should ensure that they employ effective risk management practices.

PRODUCT AND SERVICE AVAILABILITY

Wireless communication "dead zones" - geographic locations where users cannot access wireless systems - expose institutions and service providers to reliability and availability problems in some parts of the world. For some areas, the communications dead zones may make wireless banking an unreliable delivery system. Consequently, some customers may view the institution as responsible for unreliable wireless banking services provided by third parties. A financial institution's role in delivering wireless banking includes developing ways to receive and process wireless device requests. Institutions may find it beneficial to inform wireless banking customers that they may encounter telecommunication difficulties that will not allow them to use the wireless banking products and services.

DISCLOSURE AND MESSAGE LIMITATIONS

The screen size of wireless devices and slow communication speeds may limit a financial institution's ability to deliver meaningful disclosures to customers. However, use of a wireless delivery system does not absolve a financial institution from disclosure requirements. Moreover, limitations on the ability of wireless devices to store documents may affect the institution's consumer compliance disclosure obligations. [1] Additionally, any institution that opts to rely upon voice recognition technology as a means to overcome the difficulty of entering data through small wireless devices should be aware of the uncertain status of voice recognition under the E-SIGN Act. [2]

Wireless banking may expose institutions to liability under the Electronic Fund Transfer Act (Regulation E) for unauthorized activities if devices are lost or stolen. The risk exposure is a function of the products, services, and capabilities the institution provides through wireless devices to its customers. For example, the loss of a wireless device with a stored access code for conducting electronic fund transfers would be similar to losing an ATM or debit card with a personal identification number written on it. However, the risk to the institution may be greater depending on the types of wireless banking services offered (e.g., bill pay, person-to-person payments) and on the authentication process used to access wireless banking services.