

How to Use This Manual

The regulatory agencies have carefully watched and tracked the development of electronic banking and electronic commerce (e-commerce). As the volume of e-commerce increases and the number of financial institutions involved in electronic banking grows, the entire electronic banking arena is being reevaluated with respect to regulatory oversight and review. This is not only an issue in the United States; banking organizations world-wide are concerned about electronic banking on an international basis, with issues ranging from the level of controls to economic impact considerations.

Within this manual, the focus on electronic banking will take various shapes: electronic banking and e-commerce, electronic financial transactions media, or channels of e-commerce.

These are the basic categories; in the following chapters of this manual, more insights will be provided. For example, PC-based systems include PC banking, Internet, ACH, and a host of other types of banking channels. Stand-alone e-banking occurs through pre-paid cards and debit cards.

Further, the proliferation of personal computer sales to consumers and the growth of the Internet has fueled e-commerce and related changes. Given the ability to move transactions rapidly via the Internet or other electronic media, there is an increasing level of concern regarding controls and, specifically, about guarding the privacy of customers.

One recent major focus by financial institution regulatory agencies has been the importance of internal control systems. The regulators have described internal control systems within electronic banking environment as:

- The cornerstone of an effective risk management system
- Essential to an institution's management of risk
- Critical to safe and sound operations of an organization
- The foundation for safe and sound banking
- The basics to not only protect one institution, but the viability of the local, regional, national, and ultimately, world financial system.

Currently, the regulatory agencies have stated that internal control systems are weakening. Generally, the contributing factors are the:

- *Current health of the economy.* In an atmosphere of record profits, rapid growth, and numerous success stories, internal problems tend to be overlooked. This is particularly true when discussing something negative such as minor inefficiencies, data losses, unaccounted for dollars, etc.
- *Profitability of banks.* In more prosperous times, weak internal control systems can be viewed as an incidental cost of doing business. In less prosperous times, department managers may be pushed to cut staff or not fill vacancies in order to cut human resource costs.
- *Competitive environment.* As loan margins grow thinner, banks feel pressure to cut costs, introduce new products and services with minimal development time, and economize in areas they perceive as having minimal impact on income, such as internal control systems. A rush to consolidate operations and do business electronically, or offer a portfolio of products available electronically, may obscure an absence of planning and controls.

The evolution of electronic banking involves a complicated balancing of short- and long-term benefits against the risks or negatives that also arise with this change. For boards of directors and senior management teams in financial institutions across the United States, the challenges are similar. Strategies to implement electronic banking, to expand e-commerce options by making electronic products or services available to customers, and to further enhance internal technology are just a few of the issues to be considered. Technology advances also affect internal operations from security controls to database information access. What was once easily controlled by locking ledgers in a drawer and limiting access now requires a thoughtful security architecture.

Competitive Considerations

In 1998, the U.S. Department of Commerce released a report titled "The Emerging Digital Economy," which explored a number of issues regarding e-commerce. For example, the study noted that retail banking on the Internet was in its infancy. While most of the top hundred banks in the United States had Web sites, only 24 of them had truly interactive Web sites where customers could review balances, transfer funds, and pay bills. Conversely, of the study's list of 133 true Internet banks, 109 were not among the top hundred banks.

Customers clearly wanted banking online. The study noted that 4.5 million households were utilizing a dial-up connection direct to their bank or through the Internet in 1997; it projected that by 2000, from 10 to 16 million households will do their banking online.

In a 2006 Community Bank Technology Survey undertaken by Independent Community Bankers of America, BKD, LLP, CPAs, and Advisors, and Plante Moran, 83 percent noted that their organization had an Internet banking site that allowed customers to perform Internet banking transactions. The functions most frequently offered through the web sites included:

- Pay bills electronically
- Update account information
- View check images
- Apply for loans
- Apply for credit cards

The survey also noted that security is a primary focus area with the majority of respondents having specific policies to address the following focus areas:

- Acceptable Internet usage/security
- IT Disaster Recovery and Business Continuity Plans
- Data Security
- Data Security breaches
- Service Provider Selection

Of the survey respondents, 47 percent outsourced security monitoring to another company. Approximately 69 percent had an external systems/network security assessment and approximately 58 percent had an internal systems/network security assessment.

For years, there was talk of a checkless society; 2003 brought a new first to the banking industry. For the first time, electronic payments surpassed cash and checks as the consumers preferred form of payment for in-store purchases. Decreasing check volume presents an enormous growth opportunity for electronic payments. The Federal Reserve Board approved revisions/amendments to Regulation CC to implement the Check 21 Act which became effective October 28, 2004. Check 21 authorized a new negotiable instrument called a substitute check

and provides that a properly prepared substitute check is the legal equivalent of the original check for processing purposes. A substitute check, therefore, is a reproduction of the original check that meets specific legal requirements and can be processed like a check. While checks are clearly a part of the financial services system, the movement of funds is edging closer to a paperless check environment.

An Electronic Supply Chain: Will Payments Follow?

Increasingly, American consumers are making payments via electronic alternatives. Nonetheless, U.S. businesses continue to make more than 80 percent of their payments with paper checks. For some companies, creating an electronic supply chain from end-to-end offers the opportunity of linking payments to their accounting systems, permitting faster processing of invoices and payments and lessening the overall cost of the order-to-pay cycle. While an electronic financial supply chain may offer businesses some benefits, it also results in concerns pertaining to high technological costs, increased security problems, and shortened payment cycles.

The shift to electronic payments is part of the process in achieving reduced costs associated with business to business transactions. Over the past several years, solution providers and financial institutions have introduced numerous technologies aimed at enhancing business to business commerce; however, for the most part these technologies were fairly expensive and as a result only the largest firms were able to afford implementing such systems. Technological advances of late and the widespread use of the Internet have meant a broader spectrum of businesses is able to automate their respective business processes.

Regulatory Change May Help Transition

The Federal Reserve Board approved revisions/amendments to Regulation CC to implement Check 21, which provides that a properly prepared substitute check is the legal equivalent of the original check for processing purposes. A substitute check, therefore, is a reproduction of the original check that meets specific legal requirements and can be processed like a check. While checks are clearly a part of the financial services system, the movement of funds is edging closer to a paperless check environment. Check 21 guidance addresses electronic check-clearing processes, providing parameters for the use of substitute checks, and expeditious processing of financial transactions. Check 21 also addresses a wide of range of related topics including customer disclosures.

Remote deposit capture (RDC) services are provided by a bank to the customer. These services consist of providing a check scanning device, access to a browser-based software program, and all related materials and documentation that permits the customer to conduct certain check-related activities with the bank electronically. Additionally, the bank also may provide a computer to the customer upon request, whereby the customer agrees to pay a monthly fee based on the bank's current schedule of fees for such equipment.

RDC activities include the ability to scan the customer's paper checks and electronically transmit to a third-party processor, whose services are available to the bank, and for the vendor to use electronic information, including images, captured from these checks to process transactions through the automated clearing house (ACH) network. As permitted under Check 21, the equipment creates an image replacement documents (IRD). The services are provided by the bank and its vendors for access and use by customer.

Hard Dollar Investments and Staffing

The average transaction cost is only part of the competitive consideration. There are also investment considerations regarding servicing the customer. To build a branch and staff it, or to purchase/lease a site and install an ATM and service it periodically, is a significant initial investment and an ongoing staffing and servicing expense. Although Web site development can run several million dollars for a regional or multinational bank, for smaller community banks using a basic turnkey Web site product, the cost is reduced to tens of thousands of

dollars. With respect to maintenance, posting of information, changing the “look,” and other related upkeep, costs generally are less than a staffed branch or ATM site.

A Bumpy Road Exists

The changing technological environment of electronic banking and e-commerce poses distinct risks. For example, there is increasing risk in the area of privacy, such as the risk of unauthorized persons seeking the confidential and sensitive information banks gather on their customers. In addition, significant financial services industry consolidations are changing the very marketplace and competitive nature of the banking industry. This changing technological and competitive atmosphere makes now a good time for the board of directors and senior management to take a close look at the effectiveness of the institution's planning and implementation of electronic banking systems. This manual was designed to be a tool for that purpose. Whether your institution is well underway in implementing electronic banking systems, or the directors and senior management are exploring initial steps, the manual offers insights and techniques.

With industry changes projected to continue, financial institutions undoubtedly should be exploring various delivery channels and new products and services. Failure to seek new opportunities may result in future negative impact on customer bases and market opportunities that could have serious safety and soundness implications. The impact of new regulations, such as Check 21, opens the door for numerous opportunities in the electronic banking industry. It stands to reason, therefore, that financial institutions should be adding experts to staff, from in-house or by contract, to address the potential of electronic banking ideas and opportunities. Likewise, as part of this decision process, institutions should also be upgrading systems to make them more effective, secure, and resistant to tampering and intrusion.

E-Banking: Integrating and Managing Your Bank's Electronic Services has been structured to meet the needs of a variety of interests and questions within a financial institution. From the board of directors to front-line personnel, there's a role for everyone in a proactive electronic banking environment. The board of directors plays a critical role by formulating supportive policies and providing resources. Front-line staff must carry out many of the electronic banking control activities and monitoring of related internal control systems. This manual addresses electronic banking systems from the perspectives of both a one-bank entity and a multibank company.

To assist in the challenge of developing and maintaining a sound electronic banking environment, the manual offers a how-to guide that walks through various aspects of building an electronic banking system. Specifically, this manual provides management with the tools to:

- Design an electronic banking management system.
- Create a related electronic banking policy.
- Develop an appropriate formal internal control environment.
- Monitor electronic banking systems.
- Train personnel on electronic banking systems.

E-Banking: Integrating and Managing Your Bank's Electronic Services was designed to complement the earlier guides, *Data Processing Policies and Procedures: A Working Guide to Regulatory Compliance* and *PC/LAN Administrator: A Working Guide to Regulatory Compliance*. Both references are also published by Sheshunoff Information Services.

E-Banking: Integrating and Managing Your Bank's Electronic Services is the latest addition to the series of manuals addressing the technological aspects of banking. This manual can be used to write internal control corporate governance guidelines for electronic banking initiatives. Furthermore, the manual provides key insights on addressing specific electronic banking initiatives. The internal control questionnaires in this manual can be used to verify that the bank has comprehensive controls for daily electronic banking operations. Even as a stand-

alone manual, *E-Banking: Integrating and Managing Your Bank's Electronic Services* is an in-depth financial institutions emerging technology reference for your library.

Before using any of the tools in this manual, it is important to first define the term, “electronic banking.” As much as the term is used by the regulatory agencies and referred to in the press, and despite the fact that regulations address electronic banking, there is no single regulation that defines the term. As a result, the meaning of the term can vary. It is important for each financial institution to define what it means so that personnel have a common ground for understanding electronic banking systems. Such a definition will also assist in communication with external parties.

Admittedly, there is no one form or definition of electronic banking that is right for all financial institutions. What the manual covers, however, are the common critical components in electronic banking and related control systems for financial institutions. These control components were identified in various issuances and are focus areas used by the regulatory agencies. The five components are:

- Control environment
- Risk assessment
- Control activities
- Accounting, information, and communication systems
- Self-assessments

Each of these components is important to establishing a sound electronic banking program. However, the control environment is the foundation for all the others. It provides the basic discipline and structure vital to an effective electronic banking system. It also reflects the level of management commitment and awareness of the importance of all aspects of electronic banking, from initial development, to implementation, to daily operational adherence, to internal controls. It even sets the tone for the information reporting activities that are undertaken to assess how management directives are carried out. Included among formal electronic banking activities are the bank's procedures for approving and authorizing transactions and reviewing operating performance, the checks and balances limiting employees' access to assets and records, and the design and use of documents. These are critical components to ensure not only the quality of data transactions, but also the security of those transactions.

Risk assessment is the identification and analysis of relevant risk, both internal and external, that can prevent the institution from reaching its objectives or jeopardize its operations. The assessment helps determine which risks exist, how they should be managed, and what types of procedures or controls are needed to do so. This manual looks at risk from the general risk categories used by the regulatory agencies. These risk categories are:

- Credit
- Interest rate
- Liquidity
- Price
- Foreign exchange
- Transaction
- Compliance
- Strategic
- Reputation

In an electronic banking environment, a regulatory agency examiner will consider the level and range of activities, and the types of internal control systems in place to address each of these risk categories. A significant deficiency in a procedure or control will also be considered a deficiency in risk management. The bottom line is that there must be solid internal operational controls and security systems in place to effectively manage risks inherent with electronic banking. This is the third of the five regulatory focus areas listed above.

E-Banking: Integrating and Managing Your Bank's Electronic Services helps get management started with basic ideas and conceptual outlines for proposal development. An action plan and reporting mechanism are also provided to help develop and track an electronic banking initiative. Additionally, to ensure objectives are clearly set out, sample electronic banking policies, procedures, and internal monitoring questions are provided. While these examples are useful tools for determining and documenting initial efforts, including designing specific control points within the bank's internal structure, it is imperative that management review and revise them, and then adopt final policies, procedures, and control questionnaires that reflect the specific organization.

Internal controls and customer/information security are key elements for the future of electronic banking. Although the FFIEC required issuance of additional security controls methods as of year end 2006, security controls remain a primary concern of financial institution security officers and customers. Banking customers are steadily migrating to electronic online banking and bill paying; it's noteworthy to point out that surveys suggest a greater customer loyalty/openness to purchasing more banking products/services when these customers are already utilizing and are satisfied with online banking services. To assure customers that security controls are in place, it's critical that customer service representatives not only receive training in bank-specific security controls, but have the ability to discuss and explain it to customers.

The fourth component in an electronic banking program is effective accounting, information, and communication systems. These systems not only capture information and generate necessary reports, but enable all personnel to understand their roles in the overall system, how their activities relate to others, and their accountability for the activities they conduct.

Finally, the self-assessment component consists of periodically measuring and testing the effectiveness of electronic banking procedures and internal control systems. Establishing a monitoring process that is present in everyday operations can be done from information provided in this manual. Sample internal monitoring review worksheets are also a part of *E-Banking: Integrating and Managing Your Bank's Electronic Services*.

Regulatory examinations are a "fact of life" for a publicly chartered financial institution, which is insured by taxpayer funds. Any manual written for a financial institution would not be complete without including the regulatory perspective. Therefore, a chapter is devoted to regulatory examination of electronic banking activities. Tips on how to prepare for such an examination are included. In addition, an appendix includes copies of regulatory issuances, internal controls focused examination procedures, and major discussion or position documents, which emphasize the importance of internal control systems.

Banking has truly become a computerized industry. Exhibit 1.1 illustrates the various aspects of technology and its relationship to banking. With the growth of electronic banking products and services, there will be a need to further enhance computer and communication systems. The initial elements of electronic banking are only just being identified.

By reviewing and utilizing *E-Banking: Integrating and Managing Your Bank's Electronic Services*, management will be in a better position to:

- Understand the five vital components of electronic banking systems.
- Develop concepts for an institution's first electronic banking initiative.
- Sell the idea to others, including the board of directors.

- Track development and design of the new electronic banking products, services, or basic delivery channels.
- Define internal controls related to the electronic banking initiative.
- Understand the relationship of electronic banking initiatives, internal controls, and security systems to risk management.
- Perform a risk assessment.
- Design and implement security controls and procedures as well as other vital internal control systems.
- Write the institution's electronic banking activities policy and internal procedures.
- Use various discreet self-assessment methods and formal monitoring systems.
- Train staff on electronic banking and the related importance of internal control systems.
- Understand the regulatory perspective on reviews of electronic banking systems, and know what to expect from a regulatory examination.
- Modify existing electronic banking initiatives, if appropriate, to keep pace with current risk profiles of the institution.
- Be aware of trends in the industry.

Electronic Banking Controls Exist, But Who's Watching?

An operations officer at a large financial institution allegedly produced, by personal computer and with a stolen security password, bogus deposits in an account for a promotional agency at one branch. The individual did this by using the bank's computerized small business account access line and then placed the fictitious deposits into a branch account settlement process to withdraw funds from a different branch. To keep the financial institution's main computer system from flagging the imbalance, the individual created new fraudulent credits to cover the withdrawals! This fraud using microcomputer access kept the rollover going for over two years.

The interbranch settlement account was seldom reviewed for excess individual account activity, and the operations officer's usage of override codes was not challenged during this time frame. The officer also eliminated all paper certificate of deposit (CD) maturity mailings and created a limited access account status for the CDs so that the promotional agency never realized the crimes enacted through their accounts. How do you catch these types of internal fraud?

MULTI-FACTOR AUTHENTICATION

The federal regulatory agencies require each financial institution to have multi-factor authentication processes and controls in place for their e-banking programs. Institutions should work closely with their primary data processing service providers to have a multi-factor software security program that encompasses the following types of controls:

- Layered security levels reflecting different risk ratings assigned by the institution and/or customer, utilizing different authentication techniques, e.g., response to phrase, date, picture, unique identifier, or other type of question.
- Registration of customer PC location

In addition, institutions should utilize multi-level tokens. This approach facilitates access by the designated individual from different PCs. Implementing a security software package for customer e-banking access, e.g., the

software security program incorporates multi-factor authentication solution and also facilitates multi-level security for customers.

Regarding informing customers, the following are common techniques utilized to advise account holders of enhanced security procedures:

- E-mail communication
- Web site notice
- Statement stuffers
- Personalized letters and/or mailings, e.g., by name and specific account relationship
- Web site training video

In several instances, management team member point out that in preparing and implementing the multi-factor authentication controls, a major review was undertaken of internal policies and procedures. These reviews served as a process to further enhance internal controls and procedures and therefore, management commented there were ancillary benefits to the review.

EMERGING ISSUES

Due Diligence and Transparency Regarding Cover Payment Messages Related to Cross-Border Wire Transfers

The processing of cross-border wire transfers frequently involves several financial institutions. In addition to the originator's bank and the beneficiary's bank, other banks are often involved. There are circumstances where one or more of these cover intermediary banks is located in a jurisdiction other than the jurisdictions where the bank of the originator and the bank of the beneficiary are located. Consequently, cover payments are necessary. Cover payments are used by a bank to facilitate funds transfers on behalf of a customer to a beneficiary, most often in another country, but also in the same country when a foreign currency is used.

Currently, existing messaging practices do not ensure full transparency for the cover intermediary banks on the transfers they facilitate. Transparency is limited when the message format used to settle the interbank payment does not contain information about the originators and beneficiaries. Lack of originator and beneficiary information for funds transfers can hinder or limit a cover intermediary bank's ability to accurately assess risks associated with correspondent and clearing operations. As such, more detailed information regarding originators and beneficiaries of funds transfers can improve compliance with locally applicable requirements (such as the blocking, rejecting or freezing of assets of designated individuals or entities and monitoring for suspicious activity) and enhance a bank's risk management processes with respect to funds transfers.

Supervisors must be satisfied that banks develop and implement appropriate policies, procedures and processes to address respective capacities as originator banks, intermediary banks in the cover payments chain, and beneficiary banks. Supervisors may take several steps to assess their supervised institutions risk management practices with respect to cover payments. Supervisors should carefully review the risk management practices relating to those operations. Supervisors should be satisfied that appropriate internal controls are in place to monitor wire transfer activity, that these controls are effective, and that banks are in compliance with supervisory and regulatory guidance.

LISTING OF ISSUANCES AND REGULATORY GUIDELINES

The summary listing of issuances and regulatory guidelines is included in the glossary of this manual. The issuances and regulatory guidelines in their entirety can be found on the CD that accompanies this manual.

YOUR COMPANION CD

As part of your subscription to *E-Banking* you receive a companion CD. This disc contains all of the information in your print manual that shows you how to make sure your e-banking policies are established and accomplishing what they were intended to do.

Insert your CD into your desktop computer, and the Autoplay feature will assist you in navigating the files. You can search quickly and easily for specific guidance and policies.

Customize Your Policies

From electronic funds transfers to disaster recovery planning, the CD contains sample policies for your institution, checklists, examples of documentation, and clear guidelines you can use for your own policies for your operation.

You can easily customize the documents on the CD using Microsoft Word so that you keep your banking functions current with the latest compliance issues. Sample policies are provided in Chapter 6 that you can easily adapt to your institution's specific requirements.