Federal Financial Institutions Examination Council

FFIEC

Retail Payment Systems

RPS

February 2010

IT EXAMINATION

HANDBOOK

Table of Contents

Introduction

The FFIEC IT Examination Handbook (IT Handbook), "Retail Payment Systems Booklet" (booklet), provides guidance to examiners, financial institutions, and technology service providers (TSPs) [1] on identifying and controlling risks associated with retail payment systems and related banking activities. [2]

Financial institutions accept, collect, and process a variety of payment instruments and participate in clearing and settlement systems. In some cases, financial institutions perform all of these tasks. However, independent third parties are increasingly involved in this process, introducing new risks that affect the security of financial institutions. Financial institutions, acting either in consortiums or independently, remain the core providers to businesses and consumers for most retail payment instruments and services. Federal government-affiliated providers and operators, such as the Federal Reserve Banks (Reserve Banks), also compete with numerous financial institutions and private sector firms in providing various services in support of retail payments.

Recently, a number of new payment instruments have emerged that are largely or wholly electronic. Electronic payment systems offer efficiency gains by allowing for rapid and convenient transmission of payment information among system participants. However, the emergence of a new payment mechanism can also enable the rapid propagation of fraud, money laundering, and operational disruption if data is compromised. Another trend associated with emerging payments is the increased participation of nonbank third parties in retail payment systems and a lengthened transaction chain, which may increase risk in payment processes. Management of retail payments risk is increasingly difficult and requires diligent oversight of third-party service providers.

Much of the guidance in this booklet, involving traditional retail payment systems, has not been revised significantly because of the maturity of these systems in the product life cycle. Mature payment systems are better understood, whereas emerging payment systems require a closer look to better understand the risks and associated controls. New guidance is offered for remotely created checks (RCCs), electronically created payment orders, automated clearing house (ACH) transactions, The Check Clearing for the 21st Century Act (Check 21), [3] and Merchant Card Processing due to recent developments in these areas. Also, this booklet includes a new section that covers some emerging technologies in retail payment systems. Additional emphasis is placed on the need for improved operational, credit, legal, and compliance risk processes for retail payment products, especially for the deployment of remote and Internet-based check and ACH capture systems.

Examination guidance for Retail Payment Systems is provided in three sections, followed by examination procedures, a glossary, and references:

- Retail Payment Systems Overview-The first section of the booklet presents an overview of retail payment systems, grouping retail payment instruments in various categories, including: checks, card-based electronic payments, and other electronic payments, such as person-to-person (P2P), electronic benefits transfer (EBT), and ACH.
- Payment Instruments, Clearing, and Settlement-The second section of the booklet

describes the retail payment system instruments typically offered by financial institutions and the roles of various payment system participants, including third parties. Diagrams showing the typical payment flows and clearing and settlement arrangements for each of the retail payment instruments described are also included.[4]

- Retail Payment Systems Risk Management-The third section describes the risks associated with various retail payment systems and instruments, using the regulatory risk categories: reputation, strategic, credit, liquidity, settlement, legal/compliance, and operational/transaction risk. This section also presents the risk management practices financial institutions should implement in order to mitigate the risks described, and it concludes with specific controls appropriate to a number of retail payment instruments. Management action summaries for selected risks and functions are also included in this section, providing a snapshot of the risks and risk management practices described in the text.

This booklet includes a number of references to other IT Handbook booklets, including "Information Security," "Business Continuity Planning," "Audit," "Outsourcing Technology Services," "Electronic Banking," and "Wholesale Payment Systems." Also, there are references to FFIEC guidance for Bank Secrecy Act examinations that are relevant to retail payment systems and for Check 21. In addition to describing the IT risks and controls, the booklet also discusses certain credit and liquidity risks that may also be present when providing retail payment services. A full review of a particular financial institution's retail payment system environment will require an interdisciplinary team of examiners with experience in operational, credit, liquidity, and compliance risks.

Examiners should use the examination procedures for evaluating the risks and risk management practices at financial institutions offering retail payment system products and services. These procedures address services and products of varied complexity; therefore, 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 and agency-specific handbooks and guidance documents.

Retail Payment Systems Overview

Retail payments usually involve transactions between two consumers, between consumers and businesses, or between two businesses. Wholesale payments are typically made between businesses. Although there is no definitive division between retail and wholesale payments, retail payment systems generally have higher transaction volumes and lower average dollar values than wholesale payment systems. This section provides background information on payments typically classified as retail payments. The following are examples of typical retail payments. These retail payments may involve the use of various retail payment instruments or access devices (e.g., checks, ACH, card, phones, etc.).

Purchase of Goods and Services-Purchase of goods and services can occur at the point-of-sale (POS) (e.g., in person at a merchant location, through the Internet, or by telephone). These payments include attended POS payment transactions for goods or services, such as with traditional retailers, and unattended payment transactions, as with

vending machines. Increasingly, traditional retailers such as grocers and home improvement stores are using unattended payment systems at the POS as well. As technology advances, the consumer can purchase goods and services remotely without physical presence at the POS, such as via the Internet or a telephone/mobile phone. Payment instruments for retail purchases of goods and services have expanded beyond traditional vehicles (i.e., cash, checks, and credit and debit cards) to prepaid cards, contactless debit and credit cards, and other contactless devices such as key fobs, mobile phones. In addition, merchants may convert checks to electronic form at the POS, and use the ACH system for clearing and settlement.

Bill Payment-Consumers may elect to pay (or provide payment instructions for) recurring or nonrecurring bills and invoices via electronic bill payment. A particular biller's periodic recurring invoices can be electronically paid individually or set up to be paid automatically to a payment schedule. In recent years, there has been a growing trend toward payment of recurring and nonrecurring bills using Internet-based bill payment services.

P2P Payments-The vast majority of consumer-to-consumer payments are conducted with checks and cash, with some transactions using electronic P2P payment systems. The expansion of systems that permit customers to conduct P2P payments is anticipated through account-to-account (A2A) transfers, which use either the ACH or Automated Teller Machine (ATM) networks for movement of funds.

A2A Payments-With A2A payments, the consumer moves funds from his or her account at a financial institution to the account of another individual or business at the same or a different financial institution. The emerging use of the ATM networks for movement of funds may allow same day availability of funds at a cost far less than traditional wire transfer systems.

Cash Withdrawals and Advances-Consumers use retail payment instruments to obtain cash from merchants or ATMs. For example, consumers can use a credit card to obtain a cash advance through an ATM or an ATM or debit card to withdraw cash from an existing account. Consumers can also use personal identification number (PIN)-based debit cards to withdraw cash at an ATM or receive cash back at some POS locations.

Retail payment systems continue to evolve with advances in technology. These advances enable financial institutions to develop new products and services, lower the barriers to business entry for smaller institutions, and exploit economies of scale.

Recent changes in payments technology have influenced three important trends in retail payments. First, as firms seek economies of scale, the banking industry has witnessed the rapid consolidation of retail payment service providers, credit issuers, merchant acquirers, processing companies, and check processors. As a result, some small and mid-sized financial institutions have exited the business and outsourced certain functions of the retail payments process to larger financial and non-financial institutions. Nonbanks, in particular, are assuming more roles in retail payment systems such as the clearing and settlement payment functions and the issuance and processing of electronic payment cards and other devices.

The second trend is the shift from paper to electronic payments as technology has converged with the change in consumers' and merchants' preferences for convenient and low cost payment alternatives. The most significant growth is seen in debit and prepaid cards (stored value cards), followed by the increased use of Internet services like online banking and bill pay. The volume of checks and cash payments continues to decrease, with cash usage declining at a much slower rate. The emergence of new

electronic payment vehicles in the U.S. is anticipated as they are adopted in the global market.

Use of automated bill pay is a third important trend. Although consumers traditionally used checks for a large portion of bill payments in the U.S., direct bill payment through the ACH system are increasingly popular. More recently, retail firms have used check-to-ACH conversion processes to allow electronic settlement, thereby reducing the number of checks that flow through the payment system.

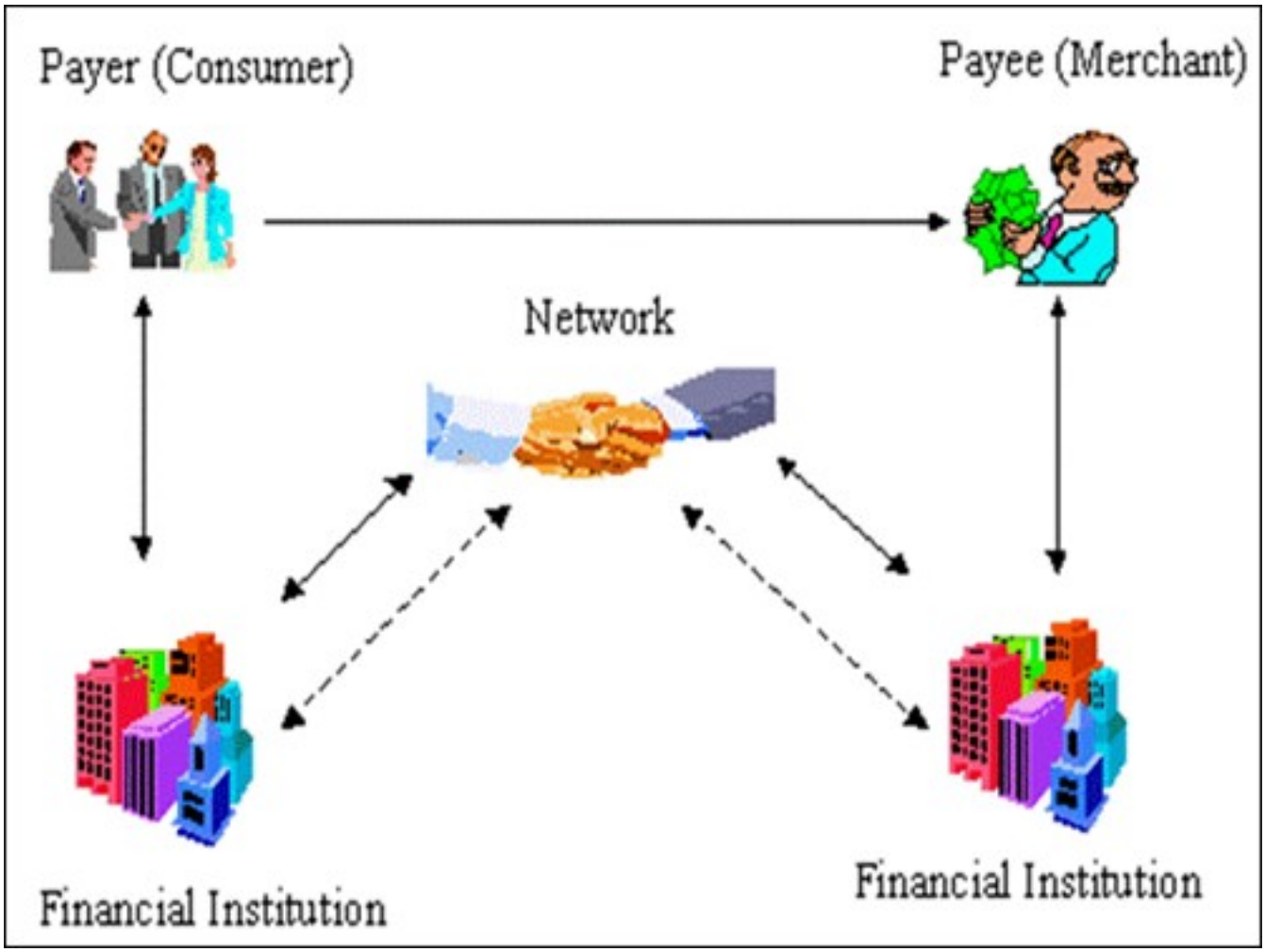
International retail payments are relatively new in the ACH industry and are largely driven by businesses and consumers seeking cost reductions for funds transfers across borders. Several financial institutions maintain their own proprietary systems, and more recently the Reserve Banks began offering FedACH International Services. FedACH International provides a means of transmitting funds between the U.S. and other countries using NACHA - The Electronic Payments Association (NACHA) rules. [5]

Beginning September 18, 2009, a new Standard Entry Class (SEC) code became effective that is expected to facilitate compliance due diligence with the use of the ACH system for international payments. The International ACH Transaction SEC code (IAT) will enable financial institutions to identify international ACH payments and perform the due diligence required by the U.S. Office of Foreign Assets Control.

Consumer and merchant acceptance of all the technological changes has been vital to the success of emerging retail payment systems and products. Consumers have shown willingness to accept new retail payment technologies more quickly because of the convenience afforded by these new services.

Payment Instruments, Clearing, and Settlement

This section provides an overview of the various payment instruments and clearing and settlement processes used for different retail payment systems. Although the diagrams reflect the general flow of transactions and participants, in many cases, other third parties may facilitate one or more processing functions.



Legend: Solid lines represent the flow of information and dashed lines represent the flow of funds.

Figure 1: Four-Corner Payments Model

Figure 1 displays the clearing and settlement process for retail payments using a standard four-corner payments model. While the flow of information and funds is different for each payment instrument, there is a common set of participants for retail payments. The initiator of the payment, typically a consumer, is located in the upper left-hand corner of the diagram. The recipient of the payment, typically a merchant, is in the upper right-hand corner of the diagram. The lower two corners of the model represent the relationship of the consumer and merchant with their financial institutions. The payments networks or clearing house organizations that route the transactions between financial institutions are in the middle of the chart. In subsequent model figures, solid lines represent the flow of information, and dashed lines represent the flow of funds. This generic figure can be applied to all retail payments.

More financial institutions are engaging third-party service providers to act on their behalf rather than keeping all payment functions in-house. In some instances, such as in check

clearing, a financial institution may exchange check items directly with another financial institution without using an intermediary.

There are a variety of retail payment clearing and settlement systems. These include; check clearing systems, ACH networks, ATM networks, and bankcard networks. Check clearing systems can be paper-based or electronic. Check 21 is facilitating the expanded use of electronic imaging technologies in check processing, enabling the banking industry to improve the efficiency and cost-effectiveness of check processing operations.

ACH payments also have grown significantly as consumers are using more direct bill payments through the ACH. More recently, retail firms have employed check-to-ACH conversion processes to obtain the efficiencies of electronic processing, reducing the number of checks that flow through the payment system.

Internet-based bill payment systems are transaction origination platforms that allow customers to initiate bill payments through existing payment systems. Depending on the bill payment software implemented, the payment transaction may be processed through ATM, ACH, or check systems. [6] The following sections describe these systems in more detail.

Debit and credit cards, particularly signature and PIN debit, have driven much of the growth in electronic payments. The recent introduction of contactless payment cards is expected to contribute to the increase of merchant acceptance and financial institution issuance of cards and investment in contactless payment infrastructure.

Retail payments often move through multiple channels, which results in data being processed and stored on multiple systems that are typically outside of the direct control of the customer's financial institution. There are two primary challenges for financial institutions in managing these complex payment systems. First, the lack of interoperability [7] that often characterizes these systems and the associated lack of optimal data protocols may result in data integrity issues. Second, the complexity of systems increases the difficulty of the management of data security and system availability.

Check-Based Payments

Checks are the traditional method that consumers can use to access their accounts. A check contains the names of the payer and the payee, the payer's account number, amount of the check, and the name and routing number of the paying financial institution. The magnetic ink character recognition (MICR) line at the bottom of the check enables high-speed reader/sorter equipment to process checks. Before financial institutions process checks, they encode the amount of the check in magnetic ink at the bottom of the check. Check formats are governed by standards developed by the Accredited Standards Committee (ASC) on Financial Services, X9B Committee, which works under procedures sanctioned by the American National Standards Institute (ANSI). [8]

Check processing has undergone a transformation during the past five years; a trend that is expected to continue for the next several years. Until recently, consumers in the United States used checks more often than any other retail payment instrument other than cash. However, in an increasing number of payment situations, checks are no longer the most convenient payment instruments for consumers, or the most cost-

effective payment method for financial institutions and merchants. Checks comprise a decreasing percentage of the total noncash payment volume in the United States. Many consumers use checks merely for person-to-person transactions that are not conducive to electronic payments, and have shifted to electronic payments for POS transactions and bill payment. In addition, a significant volume of checks are converted to ACH debits at POS and at lock-box operations.

Legal developments have affected the processing of checks as well. Check 21, which became effective on October 28, 2004, has succeeded in reducing check processing times as well as the float period previously associated with physical processing. By authorizing the use of a new negotiable instrument called a substitute check, Check 21 facilitates the broader use of electronic check processing.

A properly-prepared substitute check is the legal equivalent of the original check and includes all the information contained on the original check. The law does not require financial institutions to accept checks in electronic form, nor does it require financial institutions to use the new authority granted by the act to create substitute checks. The law permits financial institutions to truncate [9] original checks, process the check information electronically, and deliver substitute checks to financial institutions that wish to receive paper checks in lieu of electronic alternatives.

For many financial institutions, implementing a Check 21 strategy involves a significant investment in new hardware and software as well as the reengineering of check processing routines. Consequently, financial institutions should deploy Check 21 with appropriate risk management, including strategic planning, project management, and vendor management. Check 21 requires the bank [10] that creates a substitute check, the reconverting bank, to warrant that there will not be duplicate presentments of the check (or copy or representation thereof) and that the substitute check is an accurate representation of the original check as of the time the original check was truncated. Such substitute checks must meet specific requirements to be treated as a legal equivalent, and the bank that creates a substitute check must indemnify other parties for losses that result from their receipt of a substitute check instead of the original check.

Financial institutions implementing a Check 21 strategy must consider new processes for imaging checks, transferring files of imaged checks, and archiving and retrieving imaged checks. For example, a number of financial institutions are implementing remote check capture systems in their branches and processing centers as a means of significantly reducing check transit costs. Some financial institutions are providing selected customers with remote check capture devices. Examiners are encouraged to review the FFIEC's guidance for Risk Management of Remote Deposit Capture. [11]

Another important catalyst for the changes taking place in payment systems is electronic check conversion, a process in which information from a check is used to create an ACH debit. The conversion may occur at a retailer's POS, or at lock-box processing centers to which a consumer mails checks. Electronic check conversion is similar to, but separate from, the check substitution process authorized by Check 21. Instead of using the image of a paper check, as in the Check 21 process, the recipient uses the account and financial institution information contained on the consumer's check to create a new electronic payment through either the ACH or debit card networks. [12]

ACH electronic fund transfers between financial institutions are not considered check transactions; thus, they are not subject to laws governing check processing. Rather, they are governed by the rules of the ACH that processes the electronic fund transfer. ACH transactions to or from consumer accounts also are subject to the provisions of the Federal Reserve Board's Regulation E, Electronic Fund Transfers.

Evolution of Electronic Check Collection

Two general models of electronic check collection are emerging as a result of the passage of Check 21. Each model has its advantages and disadvantages. In one model, check images including the MICR payment information are transmitted to the paying financial institution. These institutions do not have to rely on multiple image archive providers (with whom they may have no direct contractual relationship) to obtain check images for customer online banking services and back-room operations.

In a second model, only the MICR information is transmitted to the paying financial institution while the check images are stored in remote archives that can be accessed on demand. The MICR information on a check could be transmitted through a dedicated network or possibly the ACH network. A small number of centralized check-image archives could be more cost-effective and might not increase risk appreciably or degrade customer service.

As electronic check collection methods evolve, efficiencies may develop to make one method superior to the other. Notwithstanding, electronic check collection methods will continue to pose certain risks. Frequently-used services that utilize both image and ACH technologies are remotely created checks (RCCs), electronically created payment orders, and remote deposit capture (RDC). Each of these is discussed in the sections that follow.

Remotely Created Checks

A closely related transaction to electronic check conversion, in that there is an authorization to debit an account, is the RCC. [13] An RCC does not bear the signature of a person on whose account the check is drawn. In place of the signature, the RCC bears the account holder's printed or typed name or a statement that the account holder authorized the check. [14] The account holder can authorize the creation of an RCC by telephone by providing the appropriate information, including the MICR data. Common examples of RCCs are those created by a credit card company, utility company, or telemarketer. RCCs may be processed through the check clearing networks or converted and processed as an ACH debit.

The risk of fraud associated with RCCs is similar to the risk associated with other kinds of debits that post to bank accounts. A fraudster might obtain an account holder's account number by copying that information from one of the account holder's authorized checks, or by tricking the account holder into providing the information over the telephone or the Internet. Once a fraudster obtains the account information, he or she has the data necessary to originate unauthorized RCC transactions through the check collection system or the ACH network. As with all payment systems and mechanisms, a financial institution must also assume responsibility for an effective system of internal controls and ongoing account monitoring related to RCCs.

For RCCs, the check and ACH rules differ as to how an accountholder receives a re-credit for an unauthorized transaction and how the loss is allocated among the participating financial institutions. ACH debits to consumer accounts are governed by applicable ACH rules and by the Electronic Fund Transfer Act and Regulation E. Unauthorized checks posted to consumer accounts are governed by check law, which includes the Uniform Commercial Code (UCC), as enacted in the applicable state, as well as the Expedited Funds Availability Act, as implemented by the Federal Reserve

Board's Regulation CC. In instances when checks are converted to ACH entries, applicable ACH rules apply.

If an unauthorized ACH debit is posted to a consumer's account, Regulation E gives the consumer 60 days after an institution transmits to the consumer a periodic account statement to report that the ACH debit was unauthorized. Regulation E imposes obligations on the consumer's financial institution with respect to error resolution procedures and refunds of unauthorized payments. When a consumer receives a refund for an unauthorized ACH debit, ACH rules permit the consumer's financial institution to recover the amount of the unauthorized payment by returning the debit item to the originating financial institution within the time permitted.

In the case of checks, a financial institution may not charge a customer's account for a check that is not properly payable from that account. The customer has a right to a re-credit for an unauthorized check so long as the customer makes the claim within the time frame permitted by the UCC and the account agreement. Unlike Regulation E, the UCC does not contain specific re-credit procedures that a financial institution must follow. With respect to the allocation of losses for unauthorized checks between financial institutions, the risk of loss falls generally on the paying financial institution, which historically has been in the best position to determine the validity of the drawer's signature. Under the UCC, a paying financial institution becomes accountable for a check unless it returns the check by its midnight deadline. [15] With the exception of an RCC, if a paying financial institution re-credits a customer's account for an unauthorized check, generally it cannot make a claim against a previous financial institution for an unauthorized drawer's signature after the midnight deadline has passed.

In response to the perceived risk of fraud, legal initiatives have shifted the risk related to unauthorized RCCs from the paying financial institution to the bank of first deposit. This shift is based on the theory that, for unauthorized RCCs, the bank of first deposit is in the best position to know its customer (the creator of the RCC) and to determine the legitimacy of its customer's deposits. A UCC revision that reallocates this risk for RCCs has not yet been widely adopted by the states. Among the states that have enacted amendments to the UCC, the definitions and warranties are not uniform in their scope or requirements. Under the pre-existing provisions of the UCC, the paying financial institution, not its customer, is responsible for unauthorized checks. Providing the paying financial institution with the ability to recover against the financial institution that presented the unauthorized RCC can make it easier for customers to obtain re-credits.

The Federal Reserve Board amended Regulation CC effective July 1, 2006, to reallocate the risk of loss resulting from unauthorized RCCs. Under the amendments, any financial institution that transfers or presents an RCC warrants that the person on whose account the check is drawn authorized the issuance of the check in the amount and to the payee stated on the RCC. The warranty applies only to financial institutions and does not directly create any new rights for checking account customers. Also, any financial institution that received an RCC from another financial institution has up to a year to make a claim against the transferring financial institution for an unauthorized RCC. Similarly, the Board amended Collection of Checks and Other Items by Federal Reserve Banks and Funds Transfers Through Fedwire (Regulation J) in 2006 to clarify that the new warranties apply to RCCs collected through the Reserve Banks. In conjunction with Regulation CC, Regulation J shifted the liability for losses attributable to unauthorized RCCs to the depository financial institution where the check is first cashed or deposited.

Because RCCs are cleared in the same manner as traditional checks, and because nothing unique identifies a check as an RCC unless the signature block on the check is

examined, there is currently no efficient way of measuring the volume or use of RCCs.

Electronically Created Payment Orders

An electronically created payment is a new retail payment practice in which a merchant takes payment instructions for goods and services and places them in an electronic template that creates an electronic file for processing through the check clearing networks. Unlike traditional checks or RCCs, electronically created payment orders do not begin with a paper item. However, they are similar to RCCs in that they are typically initiated with Internet or telephone instructions from the consumer and bear no direct evidence of the customer's authorization. Because these transactions are not originally captured from paper check items, the laws and regulations pertaining to check collection do not apply.

Ordinarily, electronic debits that a consumer uses to acquire goods or services are cleared through the ACH network, which includes a transaction code that clearly indicates the nature and source of the transaction. When a financial institution permits the creation of electronic payment orders, substantial risk-management oversight for unauthorized returns and other unlawful activity is lost because the check-clearing networks do not provide the level of technological and organizational controls of those in the ACH network. This lack of systemized monitoring of the electronically created payment orders increases the susceptibility to fraud by Web-based vendors and telemarketers.

The Federal Reserve Banks handle electronic check images only if they were created from an original paper check. On June 15, 2008, the Federal Reserve Banks revised Federal Reserve Bank Operating Circular 3 (Circular 3) [16] to clarify that a depository institution that sends an electronic check file to the Reserve Banks is liable for the legitimacy of the items in that file. Reserve Banks only accept applicable liability and offer certain warranties for Check 21 transactions that begin with an original paper check item. Because electronically created payment orders generally are indistinguishable from electronic images of paper checks, collecting banks, such as the Reserve Banks, may not be able to avoid accepting the electronically created payment orders. However, pursuant to the revised Circular 3, the bank that sends the item to the Reserve Bank ultimately assumes liabilities and provides warranties for its legitimacy.

Remote Deposit Capture

Remote Deposit Capture (RDC), the digital processing of paper checks and monetary instruments at remote locations for deposit and clearing through the check (image) or ACH networks, has expanded rapidly in recent years and is being used at financial institutions and at customer locations. [17]

Although remote deposit-taking is not a new activity, RDC should be viewed as a new delivery system and not simply as a new service. Prior to implementing RDC, senior management should identify and assess the legal, compliance, reputation, and operational risks associated with the new system. They should ensure that RDC is compatible with the institution's business strategies and should understand the return on investment and management's ability to manage the risks inherent in RDC. Management should incorporate their assessments of RDC systems, including products and services, into existing risk assessment processes.

With RDC, the depositary and collecting financial institutions may choose either to send or accept a substitute check or to engage in electronic check presentment (ECP) where data and images captured from the original checks are used to complete payment transactions. RDC includes deposit capture at the financial institution's teller line and backroom processing, at ATMs, and at customer locations. RDC at customer locations allows the customer to make deposits by scanning items on its own premises and sending either the image of the deposit item for processing through the check clearing networks or merely the deposit data for processing and clearing through the ACH network. RDC also may include the electronic capture of deposit information comprised of cash or other items such as electronic deposits made through a remote safekeeping arrangement at the customer location or through another intermediary.

Financial institutions have a greater degree of control over RDC activities deployed at wholly owned or controlled locations. Based on the RDC configuration used and on the customer's operations, RDC at a customer location increases the financial institution's legal, compliance, and operational risks to varying degrees. Legal and compliance risks could be significant depending on the effectiveness of controls and legal agreements that are in place. The use of RDC by international correspondents' customers is increasing. RDC is effectively replacing correspondent cash letter pouch activity. BSA/AML controls over RDC pouch activity should also cover RDC and should be commensurate with the increased volumes. Operational risks at the customer location include unauthorized access to technology systems and electronic data images, an inability to maintain system compatibility with financial institution systems, ineffective controls over physical deposit handling and storage procedures, inadequate record retention programs, and exposure to money laundering and fraud.

The Management Booklet of the IT Handbook and the FFIEC Bank Secrecy Act/Anti-Money Laundering (BSA/AML) Examination Manual [18] provide additional descriptions of risk management processes.

Check Clearing Houses

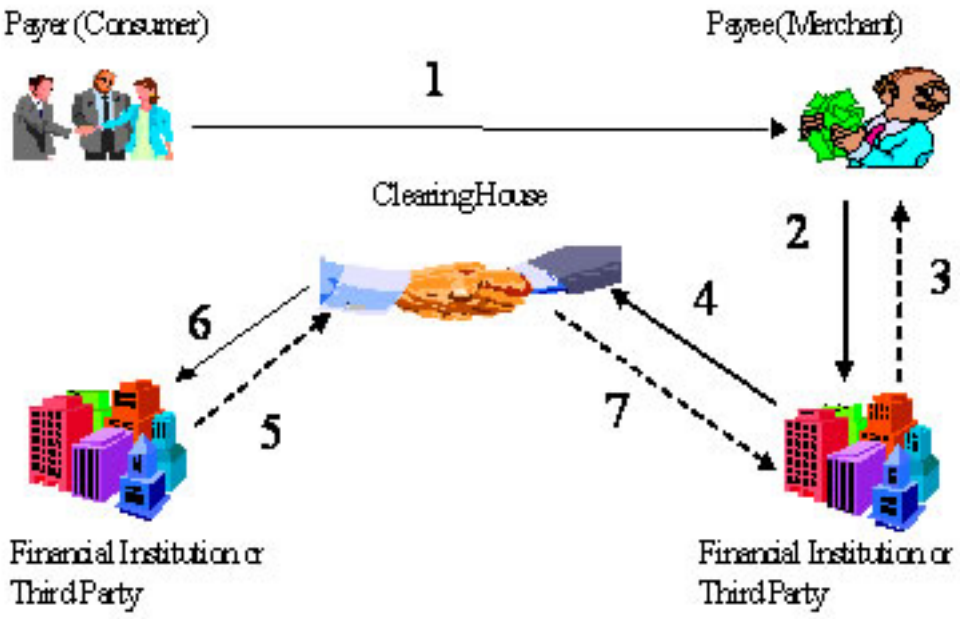
Financial institutions clear and settle checks in different ways depending on whether the checks are "on-us" (checks deposited at the same institution on which they are drawn) or interbank or transit checks (the payer and payee have accounts at different financial institutions). On-us checks do not require interbank clearing or settlement. Interbank or transit checks can clear and settle through direct presentment, a correspondent financial institution, a clearing house, or other intermediaries such as the Reserve Banks.

Under direct presentment, depository financial institutions can present checks directly to the paying financial institution. The paying financial institution may settle with the depository financial institution through a pre-arranged settlement agreement or by sending Fedwire® funds transfers through the Reserve Banks. [19]

Correspondent financial institutions, acting on behalf of other depository financial institutions (known as respondents), can settle the checks they collect by using accounts on their books or by using their Reserve Bank reserve account. Smaller depository institutions typically use the check-collection services of correspondent financial institutions or the Reserve Banks.

Financial institutions can also clear checks through a Reserve Bank or through an independent clearing house where they have formed voluntary associations that

establish an exchange for checks drawn on them. With the advent of Check 21, a number of vendors have begun to offer processes and systems for imaging, transferring, archiving, and retrieval of checks. Many financial institutions participating in check clearing houses use the Federal Reserve's National Settlement Service (NSS) to effect settlement for checks exchanged each business day. [20]



Legend: Solid lines represent the flow of information and dashed lines represent the flow of funds.

Figure 2: Check Clearing and Settlement

Figure 2 depicts the typical interbank check clearing and settlement process through a Reserve Bank or clearing house. In step 1 the consumer uses a check to pay a merchant for goods or services. The merchant, after obtaining authorization for the check, accepts the check for payment. [21] At the end of the day, the merchant accumulates the checks and deposits them with its financial institution for collection (steps 2 and 3). Depending on the location of the paying institution, the funds may not be available immediately. For deposited checks payable at other financial institutions, the merchant's financial institution uses direct presentment for processing or sends the checks to a Reserve Bank, clearing house, or correspondent financial institution (steps 4 and 6). The check or an electronic presentment file is sent to the consumer's financial institution, and the financial institution's account at the correspondent or Reserve Bank is debited (steps 5 and 7). [22]

Return items are checks that are rejected by the paying financial institution for reasons such as insufficient funds, a closed account, a stop-payment order, fraudulent signature, or failure of the paying financial institution. Return items are a major risk associated with the acceptance of check deposits. The institution that takes a check for deposit may be exposed to credit risk if it releases funds to the depositor and the paying financial institution later returns the check because its customer does not have sufficient funds or

for other reasons.

Regulation CC obligates financial institutions to make deposited funds available for customer withdrawal in accordance with mandatory schedules. Thus, a depository financial institution may be required to make funds available to the customer before an unpaid check is returned to the depository financial institution. When the depository institution receives a return item, it will charge back its depositing customer's account for the item although it had already made the funds available to the customer.

The Automated Clearing House (ACH)

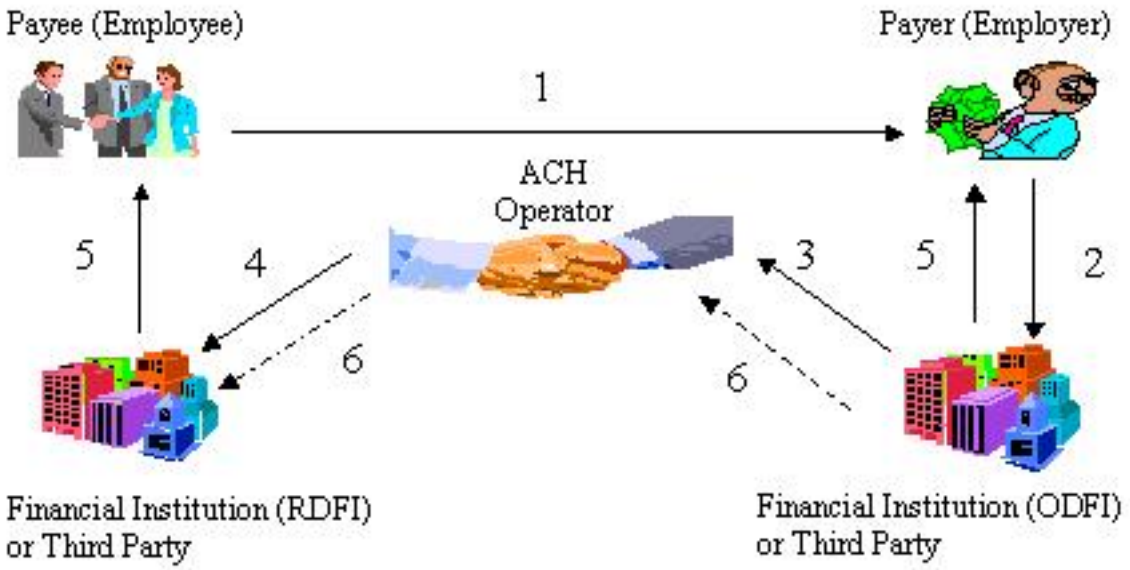
An ACH is an electronic network for the exchange of payment instructions among financial institutions, typically on behalf of customers. ACH transactions are payment instructions to either debit or credit a deposit account. They are batch-processed, value-dated electronic funds transfers between originating and receiving financial institutions. ACH transactions can either be credits, originated by the account holder sending funds (payer), or debits originated by the account holder receiving funds (payee). Financial institutions may contract with third-party service providers to conduct their ACH activities. Unaffiliated independent third parties now generate significant ACH payment activity. NACHA is responsible for the administration, development, and enforcement of the NACHA Operating Rules and sound risk management practices for the ACH Network. [23]

The ACH Network

ACH transactions are sent in batches by financial institutions and third-party service providers to ACH operators for processing one or two business days before settlement dates. The ACH operators deliver the transactions to the receiving institutions at defined times. The Electronic Payments Network (EPN), one of the two national ACH operators, is a private processor with a significant share of the national market. [24] The Reserve Banks process the remaining share of the market. ACH operators charge a small fee per- transaction to both the originating and receiving depository institutions.

In all ACH transactions, instructions flow from an originating depository financial institution (ODFI) to a receiving depository financial institution (RDFI). An ODFI may request or deliver funds. Transaction instructions and funds are linked using record keeping codes. If the ODFI sends funds, it is a credit transaction. Examples of credit transactions include payroll direct deposit; Social Security payments; dividend and interest payments; and corporate payments to contractors, vendors, or other third parties. If the ODFI requests funds, it is a debit transaction and funds flow in the opposite direction. Examples include collection of insurance premiums, mortgage and loan payments, consumer bill payments, and corporate cash concentration transactions.

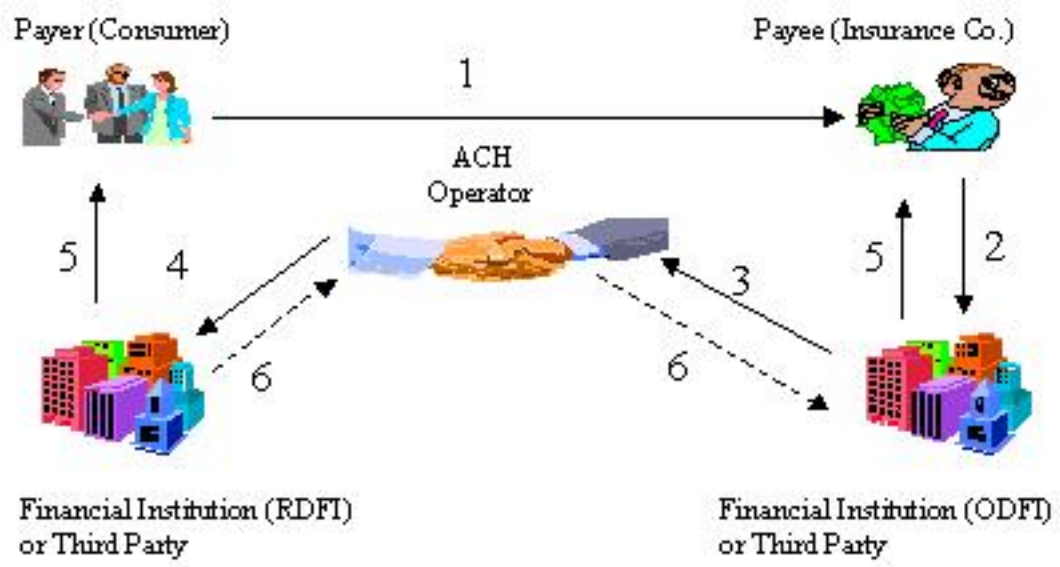
When the ACH files are distributed, financial institutions originating credit payments have a binding commitment for payment to the ACH operator. Settlement for Reserve Bank ACH credit transactions is final at 8:30 a.m. Eastern Time (ET) on the settlement day, when the credits are posted to receiving depository financial institution accounts. Settlement is final for ACH debit transactions, assuming the RDFI has sufficient funds and there are no returns, when posted at 11:00 a.m. ET on the settlement day. [25]



Legend: Solid lines represent the flow of information and dashed lines represent the flow of funds.

Figure 3: ACH Credit Clearing and Settlement

Figure 3 depicts a typical ACH credit transaction. In this example, the payer is the employer and the payee is the employee. The payee authorizes an employer to deposit his or her paycheck through direct deposit (step 1). The ODFI is the employer's financial institution and the RDFI is the consumer's financial institution. The employer submits its direct deposit payroll ACH files to the ODFI (step 2). The ODFI verifies the files and submits them through the corresponding ACH operator (step 3). The ACH operator routes the transaction to the payee's financial institution, the RDFI (step 4). The RDFI makes the funds available to the payee by crediting his or her account (steps 5). The ACH operator settles the transaction between the participating financial institutions (step 6). If the ACH operator is the EPN, final settlement is made using the Reserve Bank's NSS. If the ACH operator is the Federal Reserve, final settlement is made directly to the financial institution's reserve accounts at a Reserve Bank.



Legend: Solid lines represent the flow of information and dashed lines represent the flow of funds.

Figure 4: ACH Debit Clearing and Settlement

Figure 4 depicts a typical ACH debit transaction, in this case a recurring monthly insurance premium remittance. The payer sends the ACH payment information and authorization to the payee, in this case an insurance company (step 1). The payee submits this information to its financial institution (step 2), which routes the transaction to an ACH operator (step 3). The ACH operator routes the transaction to the receiving financial institution (step 4). Funds are made available to the payee and the payer's account is debited (step 5). The ACH operator settles the transactions between the participating financial institutions (step 6). Final settlement is performed as described in Figure 3.

An ODFI or an RDFI may outsource ACH processing functions to a third-party service provider, an entity that performs any processing functions on behalf of the ODFI, the originator, or the RDFI, including creation of ACH files or acting as a sending or receiving point. A financial institution may provide the third-party service provider with its Electronic Transaction Identifier (the institution's unique routing number that is used in the ACH network). Third-party senders, customers of the ODFI that provide services to originators, send ACH files on behalf of an originator. [26] In a third-party sender model, the ODFI does not have a direct customer relationship with the originator and must rely upon the third-party senders' warranties regarding its originators. The lack of customer knowledge of the originators poses additional risk to the ODFI.

Historically, there was little risk in the ACH system because it was a closed system with recurring transactions and relatively few originators. However, advances in technology

and changes in NACHA Operating Rules resulted in significant changes in the nature and volume of ACH activity, with the most pronounced growth being in nonrecurring payments, potentially increasing the risk of ACH transactions for both financial institutions and their customers. In addition to the primary ACH transactions, retailers and third parties use the now open ACH system for a variety of nonrecurring transactions including:

- ACH check conversion
  - Account receivable (ARC) entries. Many financial institutions operate retail lock boxes for their corporate customers as well as for their own payments collection. Lock boxes receive large volumes of check payments. With ARC, the checks are converted to ACH payments through the transmission of the MICR information on the checks. This data is batch processed for collection through the ACH network. ARC has improved the efficiency of lock-box operations by eliminating the transport of paper checks and increasing the speed of payment collection. While ARC has only been in use since 2001, in 2006 it accounted for 16 per cent of all ACH transactions and was one of the fastest growing segments of the ACH network. Recent statistics, however, indicate that ARC is currently decreasing.
  - Point of Purchase (POP) and Back Office Conversion (BOC) entries. Like ARC entries, POP and BOC entries are created by capturing the check MICR information and sending the transaction through the ACH. The most common application is with checks drawn on consumer accounts. Some retailers and third-party service providers have been converting checks to ACH transactions at the POP or during BOC. BOC was introduced in March 2007 as a new payment solution that allows merchants to collect checks in batches and convert them into debits through the ACH at a central location rather than at the POS. BOC is similar to POP and ARC in that it facilitates the conversion of consumer checks to electronic formats. BOC merely consolidates the electronic conversion process from the individual checkout lines to the back office.
- Internet-originated (WEB) and telephone-initiated (TEL) ACH payments
  - Consumers and retailers can initiate ACH transactions through the telephone and the Internet. These ACH transactions are an alternative to providing a credit card or signature-based debit card number.
- Re-presented check (RCK) entries
  - A physical check that was presented but returned because of insufficient funds may be re-presented as an ACH entry.
-

NACHA Rule and Product Changes

Over the past few years, NACHA has mandated several important rule changes to expand the use of the ACH network. Some of the more significant changes include:

- Development of a framework to support broader use of international ACH credit and debit transactions and to identify and report international ACH transactions subject to OFAC restrictions. (Effective September 2009 [27]).
- Acceptance of certain business checks for conversion to ACH debits.
- Back-office processing of eligible checks to ACH debits by retailers and billers (BOC entries).
- Use of the ACH network for presentment of bills to consumers.
- Implementation of more stringent network enforcement rules that include more substantial fines for certain violations and permit the ACH Rules Enforcement Panel to direct an ODFI to suspend an originating third party sender.
- Requirement that companies identify themselves within the ACH transaction by the name that is known to, and readily recognized by, the consumer. [28]

NACHA also requires that every financial institution conduct an annual internal or external audit of compliance with the ACH rules no later than December 1 of each year, and that the audit be made available to NACHA upon request. While the requirements for the "ACH Rule Compliance Audit" do not prescribe a specific methodology, NACHA does identify specific criteria that must be considered during the annual audits (NACHA Operating Rules, Appendix Eight). Financial institutions and third-party service providers should have processes in place to ensure their understanding of, and compliance with, these and future rule and product changes. [29]

Card-Based Electronic Payments

There is a growing array of card-based electronic payment systems available for retail use. Historically, these payments have been linked to a payee's or payer's existing account relationship with a financial institution. Card-based electronic payments can be defined in three ways, depending on the timing of the payment:

- "Pay Later" payments occur after receiving the goods or services and typically refer to credit payments. A credit card enables a consumer to access a credit line account at a financial institution.
- "Pay Now" payments occur when the goods or services are received and generally are associated with debit payments. Debit card payments are related to an existing transaction account at a financial institution.
- "Pay Before" refers to payments for goods or services with prepaid or stored-value cards, which are loaded with buying power before the purchase of goods or services occurs. The account associated with the pre-paid debit card may be the liability of a financial institution.

Both credit and signature-based debit card transactions are typically processed in batch mode at the POS, and settlement is delayed until the batches are processed at the end of the day. PIN-based debit card transactions, although processed in real time at the POS, typically settle at the end of the day using the ACH. Merchants often prefer that customers use PIN-based debit cards due to the lower costs associated with these transactions over the costs for signature-based credit and debit cards. With PIN-based transactions, the consumer must apply the pre-established PIN to validate the transaction. Each of these types of card payments is described below.

In the United States, almost all cards are magnetic-strip-based, while in Europe and Asia, consumer account information is often stored on a computer chip embedded in the card. These computer-chip-based systems have more security features than the magnetic strip systems; therefore, more financial institutions and merchants in the U.S. are adopting chip processing infrastructure. Consumers have welcomed recent initiatives with chip-based contactless cards so, the growth in these chip-based-cards is expected to continue.

In general, credit cards have revolving credit arrangements that allow consumers to make purchases and be billed later. Most credit card accounts allow the consumer to carry a balance from one billing cycle to the next and make a minimum payment in each billing cycle (e.g., two to three percent of their total balance) rather than requiring payment of the full balance.

A charge card is a specific kind of credit card that has a short-term, fixed-period credit arrangement. The balance on a charge card account is payable in full when the statement is received and cannot be rolled over from one billing cycle to the next. This arrangement exposes the issuing institution to less credit risk than open-ended accounts.

Financial institutions are important participants in various credit card systems. They issue and distribute cards, clear and settle the associated payments, and act as, or sponsor, merchant acquirers. [30] There is an increasing concentration of both credit card issuers and processors within the marketplace as larger issuers are bringing processing functions in-house. Some large institutions have exited the credit card issuance and processing businesses due to lack of economies of scale.

This booklet groups credit or charge cards in three categories: general-purpose credit cards, co-branded/affinity cards, and private label (store) cards.

General Purpose Credit Cards

General-purpose cards have the logo of one of the bankcard companies on the front. [31]

These cards are associated with the consumer's or cardholder's revolving credit account at a financial institution or other business. The revolving credit line is capped or limited based on the creditworthiness of the consumer. These cards can be used at any location that accepts credit cards from the particular bankcard company and include bankcards and closed-loop cards. Bankcards require agreements and transaction processing arrangements among participants, while closed-loop cards may not.

- Financial institutions issue bankcards in conjunction with the three major credit card

association networks, Visa, MasterCard, and American Express. MasterCard, Visa, and American Express operate "open" networks in which financial institutions can compete in card-issuing and merchant acquiring. The card-issuing financial institution and the merchant acquirer can be different organizations. Firms that serve as both the card issuing agent and the merchant acquirer issue closed loop credit cards.

Co-Branded/Affinity Credit Cards

Some merchants and organizations form marketing arrangements with financial institutions to issue general-purpose credit cards with the merchant or organization name on the front of the card. These cards are termed co-branded or affinity cards and the card accounts may be part of the bankcard company networks.

Co-branded cards typically offer consumers a rewards program. Organizations such as sports teams, schools, or service organizations issue affinity cards jointly with a financial institution that offers compensation in return for marketing to the merchant's customers or the organization's members. The institution might base its compensation on the number of account applications, the number of accounts activated, account volume and income, or other defined benchmarks.

Private Label (Store) Credit Cards

In some cases, financial institutions might issue a card jointly with a merchant. These cards are known as private label or store cards. Consumers can use them only at the merchant whose name appears on the front of the card. These cards do not carry a bankcard company logo, and the merchant typically plays a limited role in the issuance of the card or managing the credit relationship. [32]

Bankcard Companies

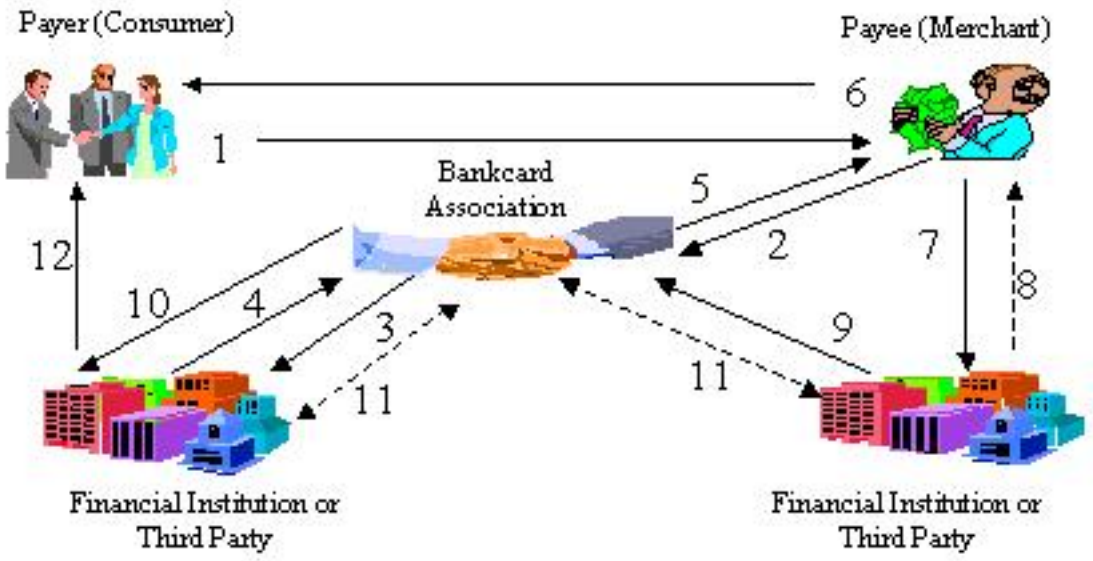
The two major bankcard companies, Visa and MasterCard, account for the majority of credit and debit cards in use. Both organizations began as bank service companies, owned by principal-member financial institutions. They provide separate, but similar operating policies, procedures, and controls for bankcard issuance, acquiring, and settlement activities. The companies own the credit card trademark, granting membership to financially sound financial institutions that apply. Only members are allowed to issue cards bearing the company logo, and they pay transaction and membership fees for use of the bankcard association logo and services.

Each company has three primary types of membership: Visa has principal, associate, and participant memberships; MasterCard has principal, affiliate, and agent memberships. Each membership type conveys different privileges. Principal membership allows members to solicit cardholders and issue cards, solicit and sign merchants, and sponsor other financial institutions for membership in the company. Associate/affiliate and participant/agent members can perform all of the principal membership functions except sponsor other members.

Card issuers are financial institutions that have permission to issue bankcard company credit cards. Acquiring financial institutions and sponsored third parties have contracts with merchants that accept a bankcard company's products. Acquiring financial institutions accept and process transactions from those merchants through the company's network interchange payment system. The cost of technology infrastructure

and the level of transaction volume are high for bankcard-acquiring institutions. Most rely on third-party service providers. [33] Under the bankcard company's bylaws, acquiring financial institutions are responsible for the actions of all contracted third-party service providers; therefore, they are expected to monitor carefully the providers' compliance with the companies' operating rules.

The bankcard companies set interchange fees, which are paid by the merchant acquirer to the issuing financial institution. The merchant acquirer typically passes this fee along with a discount or acquirer fee for processing services to its merchants. Bankcard issuing institutions generate their revenue from the interest charged on revolving balances, and from the interchange, late, over-limit, cash advance, and card fees. Merchant-acquiring institutions, which assist in clearing and settling credit card transactions, generate most of their revenue from the acquiring and other processing fees (e.g., charge-back processing and account maintenance) they charge to the merchant.



Legend: Solid lines represent the flow of information and dashed lines represent the flow of funds.

Figure 5: Credit Card Clearing and Settlement

Figure 5 illustrates the payment and information flows for a typical credit card transaction. In this example, the consumer pays a merchant with a credit card (step 1). The merchant electronically transmits the data, at the POS and through the bankcard company's electronic network, to the card issuer for authorization (steps 2 and 3). If approved, the merchant receives the authorization to capture funds, and the cardholder accepts liability by signing the credit voucher (steps 4, 5, and 6). In cases involving purchases under $25, the cardholder does not have to sign. The merchant receives

payment, net of fees, by submitting captured credit card transactions to its financial institution in batches or at the end of the day (steps 7 and 8). The merchant acquirer forwards the sales draft data to the bankcard company, who forwards the data to the card issuer (steps 9 and 10). The bankcard company determines each financial institution's net debit position. The bankcard company's settlement financial institution coordinates issuing and acquiring settlement positions. Members with net debit positions (generally issuers) send owed funds to the company's settlement financial institution, which transmits owed funds to the merchant acquirers. The settlement process takes place using a separate payment network such as Fedwire® (step 11). [34] The card issuer will then present the transaction on the cardholder's next monthly statement (step 12). The cardholder makes a payment for the charges incurred in accordance with the cardholder agreement.

Debit and ATM Cards

Debit cards are associated with an existing transaction account at a financial institution. The card enables consumers to access their accounts for a variety of transactions. Debit cards are either online (i.e., PIN-based) or off-line (i.e., signature-based).

- Online (PIN-based) debit cards have been available for several decades and have seen significant growth since the early 1990's. Online debit cards use a PIN for customer authentication and online access to account balance information. At present, financial institutions authenticate customers by matching the PIN with the account number directly through a merchant's terminal. Debit card transactions are authorized in real time at the POS using the same electronic funds transfer (EFT) networks that handle ATM transactions and are typically settled at the end of the day using the ACH network. Customers may also receive cash at the POS because messaging between the financial institution and the retailer confirms funds availability. Merchants prefer PIN-initiated card transactions as the processing fees are substantially lower. Also, credit risk is shifted to the customer as the merchant's responsibility for authentication is greatly reduced.

- Off-line (signature-based) debit cards were introduced in the late 1980's by Visa and MasterCard. Consumers are using them increasingly at merchant locations that accept bankcards. Off-line debit card systems authenticate consumers through a written signature or other authenticating action. The transactions are processed in batch mode through the same bankcard networks as credit card transactions and typically settle at the end of the business day. Generally a cardholder can use an off-line debit card anywhere that accepts a similar online transaction.

The use of biometric technology as a means to authenticate payments is also growing because of its convenience and perceived security features. Available technologies allow customers to pay for purchases by placing a finger on a sensor, which links the image to the customer's account using a simple method of finger scanning at check out. Societal implications and security concerns surrounding the use of biometric identification may act as impediments to market acceptance.

Financial institutions issue ATM cards to consumers to provide online access to account information and to allow consumers to make withdrawals and deposits at ATMs.

Consumers typically enter a PIN for authentication at an ATM, although other authentication methods such as biometric technology are available. Consumers may use an ATM deployed by other financial institutions or third parties but typically will pay fees to the ATM owner and their own financial institution. Many financial institutions now offer ATM cards that can also be used as debit cards for POS transactions at participating merchants.

Decoupled Debit Cards

Decoupled debit cards permit a financial institution to issue a debit card to consumers regardless of where their demand deposits or other transaction accounts are held. The term "decoupled" is derived from the separation of the traditional relationship between the debit card issuer and the financial institution that provides the transaction deposit account. The decoupled debit card transaction between the consumer and merchant is processed through one of the card-branded networks or an alternative proprietary network. Instead of using the EFT networks used for debit card products, the issuer uses the ACH network to debit the consumer's account for settlement.

By decoupling the debit transaction from the bank where the consumer has the depository relationship, the intermediary can capture the interchange revenue from the card transaction. A part of this product's initial appeal was the cost efficiency derived from bundling transactions prior to entry into the ACH network for settlement. However, a recent NACHA Rule Interpretation issued on November 9, 2007 [35] prohibits the aggregation of individual debit transactions prior to settlement through the ACH, and instead requires the issuer to pay ACH origination fees on each discrete transaction conducted during the course of a day. The interpretation was issued in response to concerns that bundling transactions through the ACH might mask risks that are transparent in individual transactions and unintentionally subvert risk management tools used by financial institutions that receive payment through the ACH. Decoupled debit card programs that rely on transaction bundling may need to be re-engineered to comply with the new interpretation.

The risk profile for decoupled debit card issuers differs from a debit card program because payments are settled through the ACH, creating a delay from the time the card transaction is initiated and exposing the issuer to credit risk. With a traditional debit card, a financial institution can verify the availability of funds before the transaction is authorized. With decoupled debit transactions, credit risk exposure may arise from faulty account verification or insufficient deposit account balances. Financial institutions that issue decoupled debit products should implement risk management programs to mitigate and control these new risks associated with the nontraditional customer relationship.

EFT/POS Networks

EFT/POS networks process, route, clear, and settle ATM and online POS debit card transactions by linking financial institution card issuers and merchant acquirers, consumers, merchants, and third-party service providers through telecommunication gateways. The primary functions of the networks include routing transactions through central switching gateways, acting as clearing houses to settle network member on-us transactions, and forwarding "foreign" nonmember transactions for processing. Both credit card and signature-based debit card transactions are processed in batch mode at the POS, and settlement is delayed until the batches are processed at the end of the day. PIN-based debit card transactions typically settle at the end of the day using the ACH, although they are authorized in real time at the POS.

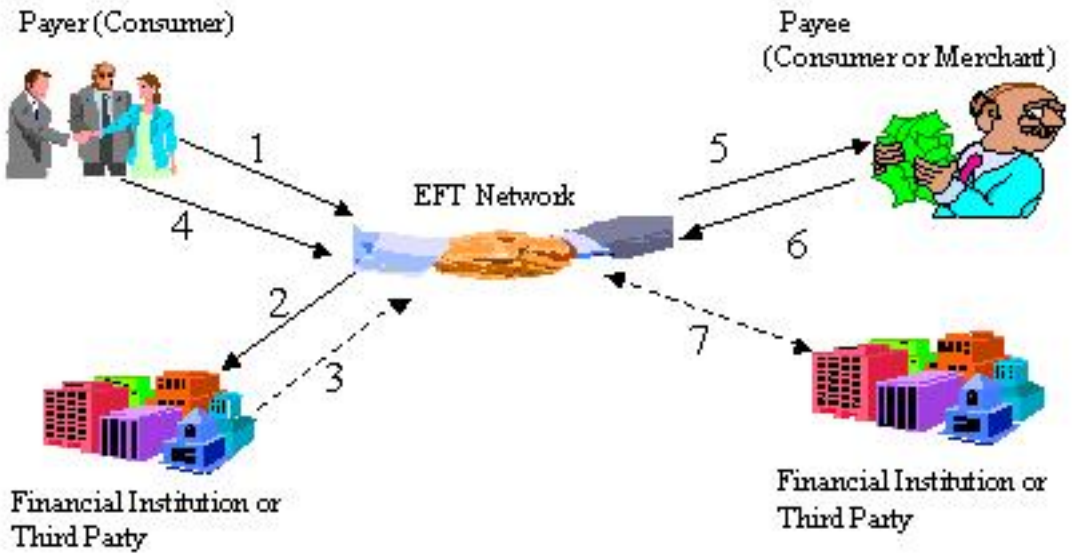
Most financial institution and nonbank ATM networks are connected to regional and national EFT/POS networks. Most regional EFT/POS networks are joint ventures owned and controlled by competing financial institutions, some function as cooperatives, and some are owned and operated by a single firm as a profit-making enterprise.

Visa and MasterCard own and operate the two national EFT/POS networks: (1) Visa's Plus and MasterCard's Cirrus ATM networks, and (2) Visa's Interlink and MasterCard's Maestro POS networks. The national networks serve as a bridge between regional networks, allowing them to route transaction information among them.

Membership in regional and national EFT/POS networks facilitates universal access to financial institution card-based electronic services and provides participant financial institutions with an interchange system offering authorization, clearing, and settlement services. Acquirers collect interchange fees from network members (issuers) to cover operating costs. With ATM transactions, the issuer pays fees to the acquirer, in contrast to credit and debit card networks in which the acquirer pays fees to the issuer.

Many financial institutions often rely on third-party service providers to conduct ATM and debit card payment processing. Third-party service providers provide a range of retail payment-related services, including card issuing, merchant, account maintenance and authorization, transaction routing and gateway, off-line debit processing, and clearing and settlement services. Although merchant acquiring financial institutions may use third-party service providers to perform many acquiring activities, the acquiring financial institution remains responsible for all third-party service-provider merchant activities.

Independent sales organizations (ISOs) provide third-party services to install and operate ATM and POS terminals for financial institutions and merchants. Representing merchants and community financial institutions, an ISO typically contracts with third-party service providers for a variety of services including support of ATM and POS terminals, transaction processing, and cash restocking. Some EFT/POS networks require an ISO to be sponsored by a financial institution member of the network.



Legend: Solid lines represent the flow of information and dashed lines represent the flow of funds.

Figure 6: PIN-based Debit Clearing and Settlement

Figure 6 describes a generic, online, PIN-based, debit card transaction. The consumer enters a PIN to authorize the transaction (Step 1). The merchant's financial institution requests authorization from the consumer's financial institution through the EFT/POS network (Step 2 and Step 3). The consumer's financial institution, or in some cases the regional network, verifies availability of funds and debits the consumer's account (step 4). The EFT/POS network contacts the merchant and authorizes the purchase (Step 5).

Typically, the acquiring financial institution does not credit the merchants' account with the entire amount of the transaction (similar to credit card clearing). Rather, the merchant receives the transaction amount, net of applicable fees and other expenses assessed by the acquiring financial institution and other intermediaries to the transaction (Step 6). For settlement, at the end of the business day, the regional EFT/POS networks determine the net debit and credit positions of the participating financial institutions and settle their positions using the ACH (Step 7).

Prepaid (Stored Value) Cards

The market for prepaid cards, sometimes called stored value cards, is one of the fastest growing segments of the retail financial services industry. While the terms prepaid cards and stored-value cards are frequently used interchangeably, differences exist between the two products. Prepaid cards are generally issued to persons who deposit funds into

an account of the issuer. During the funds deposit process, most issuers establish an account and obtain identifying data from the purchaser (e.g., name, phone number, and etc.). Stored-value cards do not typically involve a deposit of funds as the value is prepaid and stored directly on the cards. Because its business model requires cardholders to pay in advance, it substantially eliminates the nonpayment risk for the issuing financial institution. The functionality of this product is leading to a wide range of card programs that operate in either closed or open-loop systems, and program innovation has resulted in the development of systems that operate in both structures. Closed-loop systems are generally retailer/issuer business models, while general-purpose cards issued by financial institutions tend to operate in open-loop systems. Open-loop system prepaid cards are processed using the same systems as the branded network cards - MasterCard, Visa, American Express, and Discover - and offer the same functionality.

In the past, prepaid cards were mostly issued by nonfinancial businesses in limited deployment environments such as mass transit systems and universities. In recent years, prepaid cards have grown significantly as financial institutions and nonbank organizations target under-banked markets and overseas remittances. Technological innovations in the way information is stored (e.g., magnetic strip or computer chip), the physical form of the payment mechanism, and biometric account access and authentication are converging to create efficiencies, reduce transaction times at the POS, and lower transaction costs.

There are several types of prepaid cards, including gift, payroll, travel, and teen cards. Either the consumer or an issuer funds the account for the card. When a consumer uses the card to make a purchase, the merchant deducts the amount of the purchase from the card. Transaction authorization can take place through an existing network, a chip stored on the card, or information coded on the magnetic strip. Once the stored value in the card is exhausted, customers may either replenish the value or acquire a new card.

In addition to cards, stored-value payment devices are emerging in a variety of other physical forms, most notably key fobs. With the recent introduction of contactless payment technologies, use of chips (smart cards), radio frequency identification (RFID), and near field communication (NFC) payment devices are becoming more innovative. Initiatives are underway to introduce mobile phones with integrated microchips that can initiate a payment when waved over a specially-equipped reader. The integrated chip can store value, authenticate a consumer, or contain consumer preferences and loyalty program information that can be used for marketing purposes.

Prepaid cards may be subject to legal and regulatory risks. For example, the Federal Reserve Board's final rule on Regulation E, issued August 30, 2006, extended its applicability to prepaid cards used for consumer's payroll. The Federal Reserve Board noted that it will monitor the development of other card products and may reconsider Regulation E coverage as these products continue to develop. State laws vary widely with regard to fees. Additionally, financial institutions should ensure that prepaid card product programs comply with the BSA and anti-money laundering guidance.

Payroll Cards

Payroll cards provide a means for paying a consumer's wages or other compensation in an access device with the functionality of a debit card. The card is loaded with the customer's payroll information on a magnetic strip or microchip and can be used to access an account that the employer establishes with a financial institution. The

employee can use the payroll card to withdraw the funds at an ATM and to make POS purchases without a banking relationship. Some payroll cards may offer features such as convenience checks and electronic bill payment. Payroll cards are often marketed to employers as a cost-effective means of providing wages to employees who lack a traditional banking relationship. Their low-cost structure and debit-like functionality make them attractive as an alternative to direct deposit to more transient consumers. The Federal Reserve Board has amended its Regulation E to apply to payroll cards.

Payroll cards are supported by the Visa and MasterCard networks and can be used in every way that other branded cards are used. Employers are increasingly adopting payroll cards, and the growth is expected to continue because of their cost advantage to employers and financial institutions. Third-party service providers have sought opportunities in this market and may be engaged for card issuance, processing transactions made on the payroll card account, providing a range of program administration services for financial institutions or employers, and offering customer services to cardholders. Figure 7 illustrates the various relationships in an open-system payroll card program.

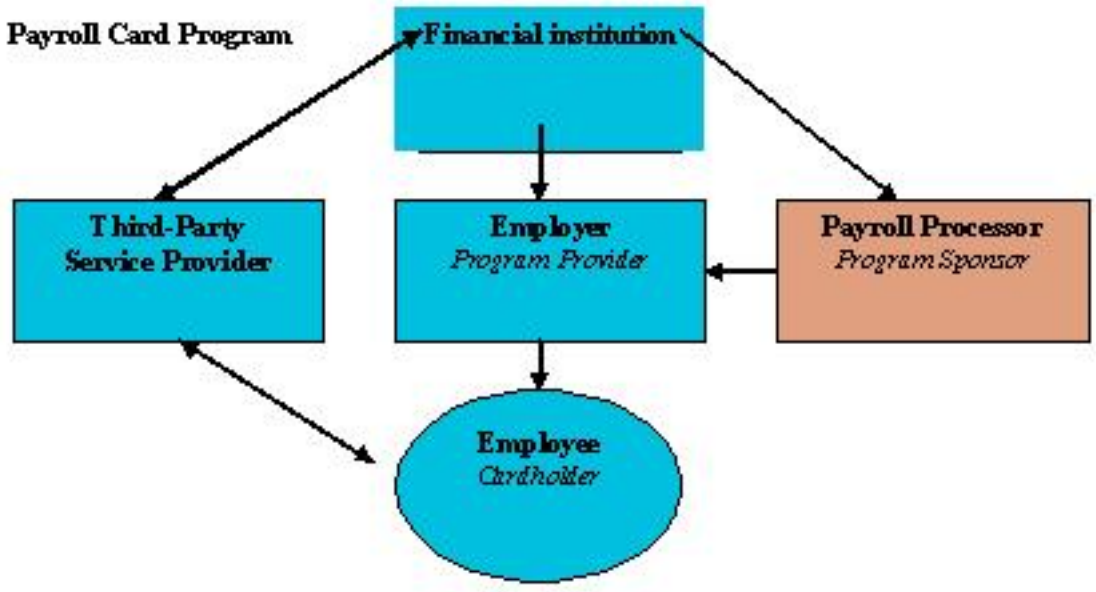


Figure 7: Open-system payroll card program

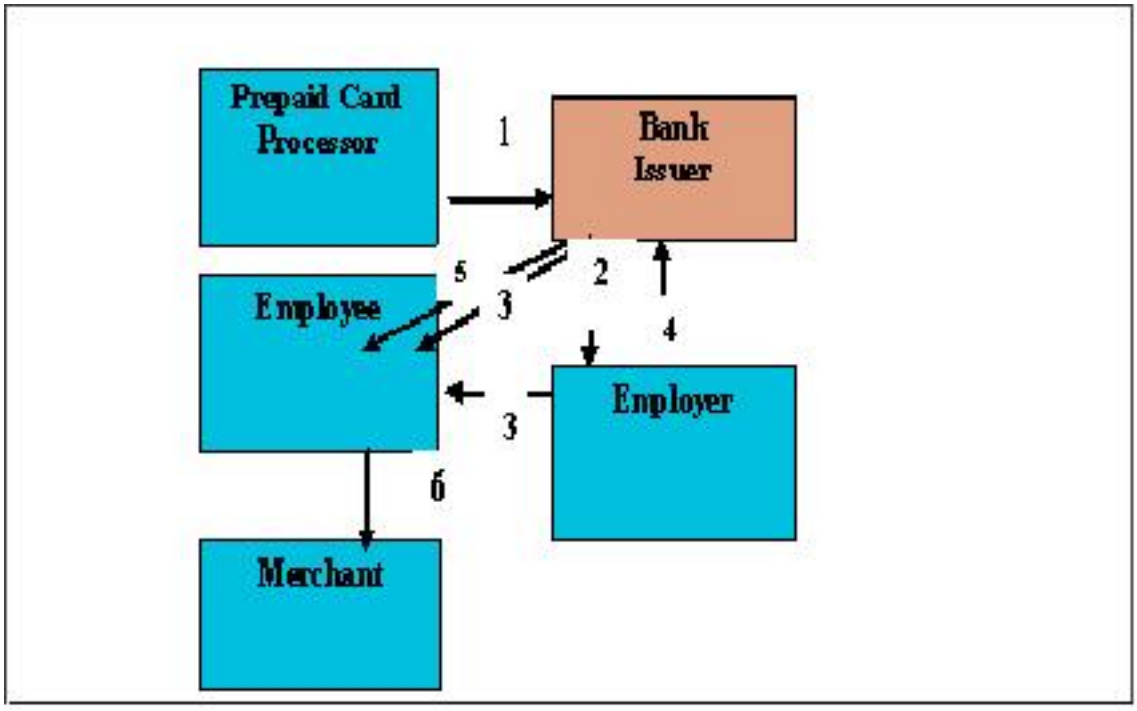


Figure 8: Stored value card product designed for corporate payrolls

Figure 8 describes a stored value card used in a payroll program. A stored value processor works with a financial institution to establish a payroll card program (Step 1). The issuer (financial institution) manages the card issuance and transaction processing. The financial institution offers the payroll card services to employers (Step 2). Either the financial institution or the employer distributes the payroll cards to employees (Step 3). The employer tells the financial institution the amount to credit to each employee's payroll card account (Step 4). On the pay date, the financial institution posts the funds to the employees' accounts (Step 5), allowing them to make purchases at any merchant that accepts the card's branding, e.g., Visa, MasterCard (Step 6).

General Spending Reloadable Cards

General spending card programs are offered by both financial institution and nonbank program providers or sponsors and are typically targeted to a particular consumer segment. Nonbank program providers usually sell this type of card and may have a relationship with a money service business or retailer, who, in turn, acts as agent for a nonbank program provider. See Figure 9 for a typical structure. Check-cashing businesses and convenience stores are examples of agents used by nonbank program providers. All network-branded prepaid cards must be issued by a partnering financial institution that is a member of the Visa or MasterCard networks or by American Express or Discover. There is a growing group of market participants associated with these programs and a developing range of potential functionality.

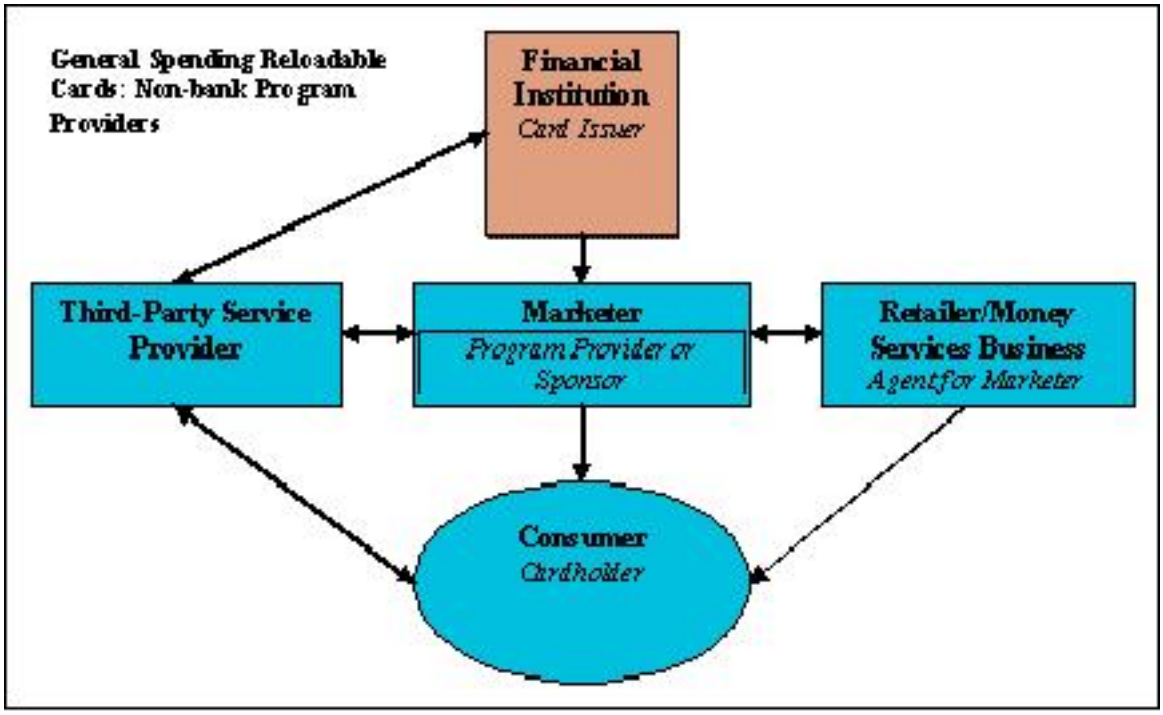
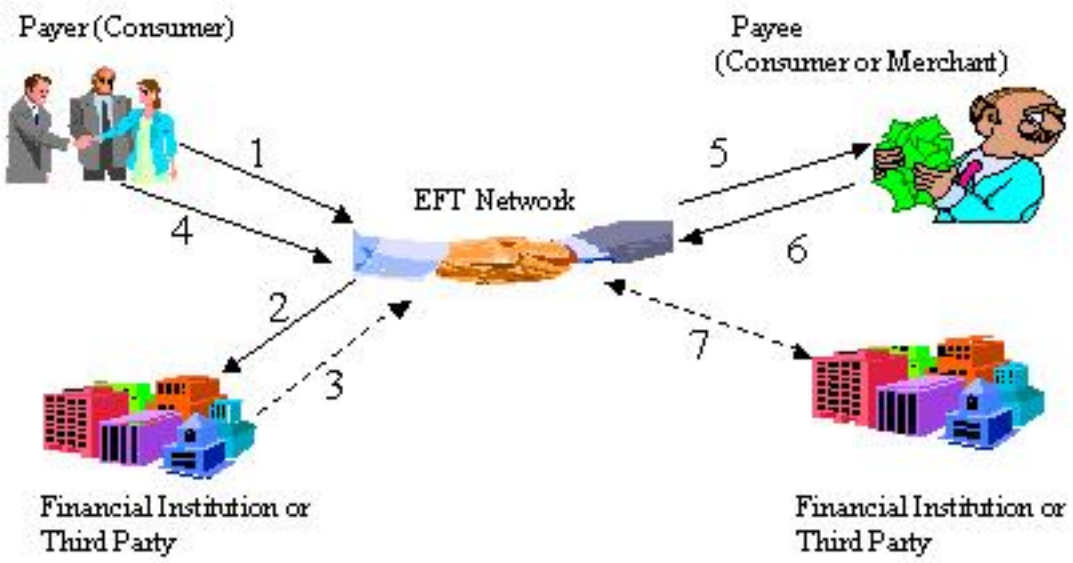


Figure 9: General spending card program offered by nonbank providers

Prepaid card transactions typically follow the "four corner" pattern in Figure 10. The consumer purchases a prepaid card (Step 1 and Step 2). When the consumer pays for goods or services with the card, electronic notations or tokens transfer from the card to the merchant's cash register (Step 3, Step 4, and Step 5). The merchant contacts the computer network of the financial institution that issued the prepaid card and presents the tokens for payment (Step 6). The network notifies the consumer's financial institution to pay the appropriate sum to the merchant's financial institution, and net settlement occurs at the end of the business day (Step 7). The financial institution keeps a percentage of the payment (the discount) as compensation for the services provided.



Legend: Solid lines represent the flow of information and dashed lines represent the flow of funds.

Figure 10: Stored Value Card Clearing and Settlement

There are many configurations of third parties and financial intermediaries, and there is a significant number of prepaid cards in circulation for which the four-corner diagram is not sufficient. The financial intermediary may hold the funds supporting the circulating stored value in a pooled account, with a third-party keeping the record of the individual transactions. Financial businesses that are not traditional financial institutions may be the issuers and may distribute the cards through retailers.

If the prepaid card is not a smart card, the associated funds are kept in a separate account. When a customer uses the prepaid card, the merchant sends a message to the record-keeping entity to determine whether the balance is sufficient to cover the transaction. If funds are available, the third party or financial institution processes the transaction.

This account arrangement may be used for smart cards also, with the accounts debited when the merchant presents tokens for payment. Although financial institutions issue prepaid cards and maintain account records, third parties may be involved in maintaining individual account records also.

Three general-spending prepaid card programs that increasingly are offered by financial institutions include branded remittance cards, teen cards, and gift cards.

Remittance Cards

With the growing demand for global person-to-person money transactions, an increasing number of bank-issued cards are being used to make remittances. In many cases, the sender of the remittance lives in the U.S. and uses a financial institution to electronically transfer money to a pre-established, branded prepaid card account. A financial institution in the sender's or recipient's country issues a prepaid card to the recipient. The recipient can use the card to obtain cash at an ATM or goods and services at a merchant POS. Alternatively, the sender may use a branded prepaid card to send funds to a recipient via the Internet. The recipient receives the funds either in cash or in credits made to an existing prepaid card account or a bank account.

Teen Cards

Another stored-value product gaining favor among consumers is the teen card that is marketed to help parents instill financial responsibility in their children while monitoring and supervising their spending. The consumer typically funds the prepaid card with the issuing financial institution through a withdrawal from a deposit account or by charging a credit card.

Gift Cards

Gift cards were initially offered by retailers as a replacement for paper-gift certificates and operated in closed-loop payment systems. In recent years, financial institutions noted the rising popularity and market potential and included gift cards in their product offerings thereby competing with retailers. Gift cards issued by a financial institution typically are card network branded and operate in an open-loop payment system, making them functional at ATMs and at any POS that accepts network debit and credit cards.

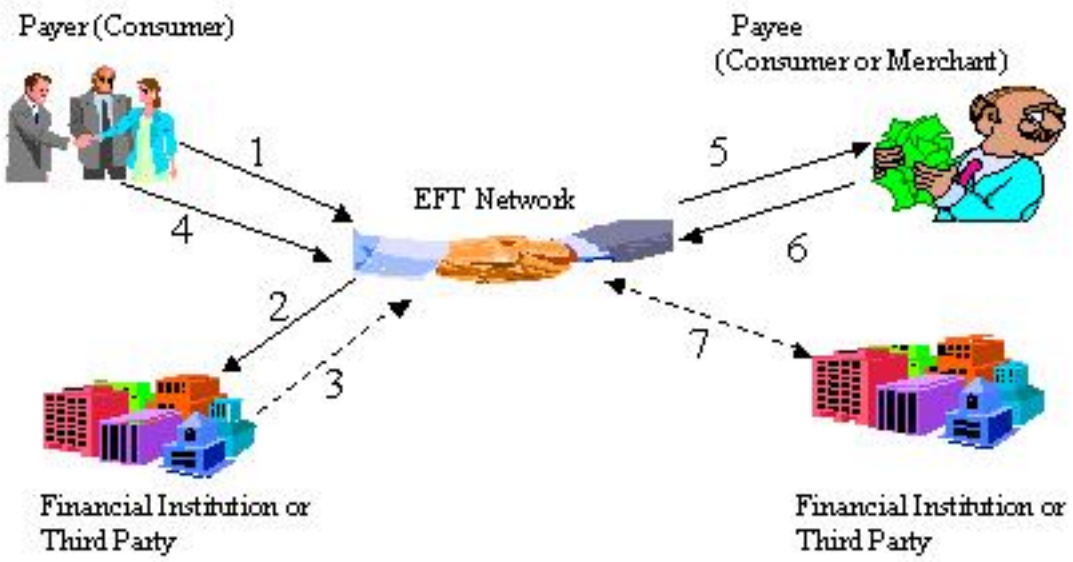
Online Person-to-person (P2P), Account-to-Account (A2A) Payments and Electronic Cash

Other electronic payments include person-to-person, account-to-account, electronic cash, and electronic benefit transfers. These payment instruments are usually associated with an established consumer deposit account and facilitate consumer access to recurring or one-time debit and credit transactions and a variety of federal, state, and local government benefit programs.

Online P2P or e-mail payments typically use traditional payment networks to transfer funds electronically from one consumer to another. Though these payments are named for their ability to send funds among individuals online, the majority of P2P payments are Internet purchases at online auctions or small businesses. In most cases, P2P transfers use existing retail payment systems to add and withdraw funds from accounts. The simplest case is when the person making a payment and the receiver maintain accounts at the same bank. This type of payment is called an "on-us" transaction. They are settled by posting accounting entries on the books of one financial institution. P2P transfers also may occur outside the traditional payment networks and, in their simplest form, may take place as an exchange of cash between two individuals. As technology advances, the transfer of funds through the use of proximity devices, such as mobile telephones and personal digital assistants (PDAs), is likely.

Most P2P services charge to the receiver of the funds a fee that varies depending upon

various factors, including payment method and the sender's credit history. Payments made with funds that originated from either ATM or ACH transactions are less expensive than payments made with funds originated from credit cards. P2P systems may offer to the receiver an opportunity to obtain funds through a check and for an additional fee.



Legend: Solid lines represent the flow of information and dashed lines represent the flow of funds.

Figure 11: Online P2P Clearing and Settlement

Online P2P payments typically occur using the process described in Figure 11. The sender of the funds must have an account with the P2P service provider (Step 1). Depending upon the service, the funds may come from an existing credit card or transaction account or may be drawn from a previous balance with the online P2P payment provider (Step 2 and Step 3). The sender can designate the e-mail address of the intended funds recipient (Step 4). The P2P network transfers the funds to the receiver's account as an "on-us" transaction. Once the funds reach the receiver's account, notice of the transaction is sent through e-mail to the receiver (Step 5). The receiver of the funds must join the service if it does not already have an account (Step 6). The online P2P payment service can disburse the funds from the receiver's P2P account through an ACH payment, a check payment, an EFT credit, prepaid card, or a credit to a credit card account (Step 7).

Account-to-account (A2A) payments are similar to P2P payments. They involve the transfer of funds from one customer's account to another account at either the same or another financial institution. Like P2P payments, A2A transfers can be initiated through the customer's Internet banking service, a biller's payment Web site, or by telephone instruction from the customer. Unlike P2P transfers, consumers must access an existing

retail payment account (deposit account) at a financial institution in an A2A transaction. To complete a transaction, the customer must know the recipient's account number or some other identifier. A2A payments can be effected on the ACH or ATM networks. On the ACH networks, funds are cleared and settled within two to three days. The ATM networks may allow same-day funds availability although settlement may not occur for two or three days. Same-day transfers using the ATM networks are usually less expensive than traditional wire transfers.

P2P payments are a growing segment of the A2A market. The success of the P2P online auction model is attributed to the consumers' demand for convenient and reliable P2P transactions. P2P payments may include transaction accounts and may be conducted through the use of proximity devices such as mobile telephones or PDAs. P2P payments are expected to grow as more reliable and convenient payment methods are introduced.

Financial institutions and retailers are also developing electronic cash-payment instruments. Similar to P2P payments, individuals can transfer electronic cash value to other individuals or businesses, generally through the Internet. Consumers can use the cash payment instruments for purchases at retailers' Web sites or they can transfer cash to other individuals through e-mail. Pre-funded accounts that consumers can use for online auction payments are among the most recent applications. In these applications, individuals use a credit card or signature-based debit card number to pre-fund the Web certificate or electronic account, and recipients redeem the value from the issuer.

Electronic Benefits Transfer (EBT)

EBT systems allow recipients of government benefits to authorize transfers from their benefits accounts to health care providers and retailers. The federal government and several states routinely use these accounts to issue food stamps and other benefits. The government distributes all food stamp benefits using this technology and, while the average transaction value is low, total transaction volumes are significant. The institution holding the account authenticates transactions using PIN technology. EBT programs now use cards with either magnetic-strip or microchip technology. Since cards using chip technology have larger storage capacities than cards with a magnetic strip, they can handle more complex transactions. Security measures can be encoded on the card strip or microchip as well to help prevent unauthorized use.

Emerging Retail Payment Technologies

This section discusses several emerging retail payments technologies that financial institutions are implementing or considering. The success of emerging retail payment methods depends upon four key drivers: reliability, cost, convenience, and speed. In terms of the preferences by consumers, merchants, and payment processors, the key drivers are technological advances, convenience, and lower transaction costs. The evolution of such preferences is facilitated by traditional financial institution relationships and established payments networks and infrastructure. Internet, mobile, and contactless payments may be used alone or together to facilitate electronic transactions, further reducing the use of paper checks. The use of currency is expected to retain some appeal because of its anonymity; however, the substitution of electronic payment vehicles for cash micro payments (transactions under $5.00) is expected to increase.

While the environment for emerging payments is highly dynamic, the most important

emerging payments today are electronic bill presentment and payment (EBPP), P2P, A2A, and stored-value instruments. Several more recent emerging payment mechanisms are contactless payments, biometrics, and proximity payments as well as the format and transmission mechanics used to effect these payments.

Contactless Payment Cards, Proximity Payments and Other Devices

Contactless cards and key fobs have an embedded computer chip with financial and personal information used for payment transactions, and they employ RFID technology for payment transmission. The contactless cards include a microcontroller (or equivalent intelligence) and internal memory and have the ability to secure, store, and provide access to data on the card. The microcontroller also supports the use of improved security features including authenticated information access and information privacy. Traditional plastic cards are easily transitioned to these new contactless cards. Other smart-card technologies provide similar capabilities but do not have the radio frequency interface that would enable them to be read quickly and conveniently at a short distance from the reading mechanism.

Proximity payments are POS transactions made with a mobile device like a cellular telephone, smart card, PDA, or virtually any device that can house a microchip. If the payment is executed with a mobile phone, it may be referred to as an M-payment. Proximity payments are faster, cheaper, and easier than traditional payment mechanisms such as cash or credit card type transactions, particularly for micro payments. Many of these transactions use the same credit/debit card network, and provide lower costs to institutions and to merchants.

Proximity payments and contactless cards permit the consumer to maintain physical control of the access device rather than relinquishing such control to an operator at a POS. Bankcard companies and governmental agencies have become the leaders in facilitating these transactions. Currently, there are multiple transmission types in use, and several are discussed below. Other transmission types are undergoing market test trials.

Financial institutions offering advanced payment technologies (i.e., commercial POS systems to merchants or consumer proximity devices) need to perform the same due diligence and vendor management as they would on any service provider. This includes ensuring an appropriate level of security in the devices.

Biometrics for Payment Initiation and Authentication

Biometric payment services allow a consumer to make purchases or to cash checks using a biometric identifier such as a finger scan linked to his or her personal identification information, accounts at a financial institution, or loyalty programs. Other biometric methods include voice scanning and iris and retinal imaging. Biometric technologies are used increasingly for consumer account authentication. However, a biometric identifier alone is only a single factor, and it may need to be combined with other technologies or factors for proper authentication of high-risk banking transactions. [36] FFIEC Guidance "Authentication in an Internet Banking Environment - Supplement," June 2011 www.ffiec.gov/press/pr062811.htm As new payment systems emerge, industry demands for anti-fraud measures may result in greater use of biometrics.

Emerging Network Technologies

The previously discussed emerging payment systems rely upon, and may be integrated with, underlying network communication technologies and protocols. If not properly implemented, new and emerging network communication technologies may expose the payment device or system to additional vulnerabilities. This is particularly true with any network that relies upon broadcast technology to send and receive information. Even close proximity wireless devices, such as RFID, have been found to be vulnerable to eavesdropping at distances greater than they were designed for. Care should be taken to ensure that the underlying network communication technology has security appropriate to the information being transmitted. Currently, there are four types of short-range wireless connectivity technologies that can be used to connect payment devices to POS devices. These include: Infrared, RFID, NFC, and Bluetooth.

Infrared

Infrared communication technology works similarly to a television remote control as information is sent from a device to a payment terminal via a frequency that is invisible to the naked eye. These devices can have signals that are stronger than other contactless technologies and can work from several yards away. Security concerns arise regarding the ability to compromise a transmission because of the strength of the signal. This concern is somewhat mitigated because there must be a direct line of sight for the transmission to work. The Infrared Financial Messaging Group (IrFM) is a consortium of technology and financial companies (including Visa) that work together to promote uniform and interoperable standards [37] for infrared devices. These standards include encrypted channels.

Radio Frequency Identification

RFID is a method of remotely storing and accessing data on devices called RFID tags/ transponders. An RFID tag can be incorporated into a plastic card (as with contactless cards), a fob, or other device. RFID tags also can be embedded into any product to track inventory. RFID tags contain antennas that enable them to communicate via radio frequency with an RFID transceiver. The technology protocol most widely used for RFID is the ISO 14443 standard. This standard is very general and can be used for multiple types of media and a broad range of hardware.

Near Field Communication

NFC is another short-range communication technology similar to RFID, but based on the ISO 18092 standard. NFC chips can be embedded in a mobile device such as a telephone to enable it to act as a contactless payment card. NFC has additional functionality such as the ability to act as a reader of other NFC devices, thus enabling two consumer devices to share data or transact payments with each other. NFC chips can also be integrated with other applications within the mobile device to permit transactions from multiple accounts.

RFID and NFC have become very flexible solutions for alternative payments. Financial institutions are adding RFID tags to credit and debit cards to speed transactions. In some parts of the world, consumers can link their credit or debit accounts to cell phones enabled with RFID or NFC technology to make purchases at retail sites equipped with payment readers.

Bluetooth

Bluetooth is a close-range wireless radio frequency communication protocol that has been implemented in a wide range of technologies. Bluetooth uses a stronger signal than RFID or NFC and is detectable at greater distances. There has been limited adoption of this protocol.

Retail Payment Systems Risk Management

Action Summary

Financial institutions engaged in retail payment systems should establish an appropriate risk management process that identifies, measures, monitors, and limits risks.

Management and the board should manage and mitigate the identified risks through effective internal and external audit, physical and logical information security, business continuity planning, vendor management, operational controls, and legal measures.

Risk management strategies should reflect the nature and complexity of the institution's participation in retail payment systems, including any support they offer to clearing and settlement systems. Management should develop risk management processes that capture not only operational risks, but also credit, liquidity, strategic, reputational, legal, and compliance risks, particularly as they engage in new retail payment products and systems. Management should also develop an enterprise wide view of retail payment activities due to cross-channel risk. These risk management processes should consider the risks posed by third-party service providers.

Financial institutions should tailor their risk management strategies to the nature and complexity of their participation in retail payment systems, including any support they offer to clearing and settlement systems. Financial institutions must comply with federal and state laws and regulations, as well as with operating rules of clearing houses and bankcard networks. From the initiation of a retail payment transaction to its settlement, financial institutions are exposed to certain risks. For individual retail payment transactions, risks resulting from compliance issues and potential operational failures including fraud are always present. Operational failures can increase costs, reduce earnings opportunities, and impair an institution's ability to reflect its financial condition accurately. Participation in retail payment systems may expose financial institutions to

credit, liquidity, and operational risk, particularly during settlement activities. In addition, a financial institution's credit, liquidity, and operational risks may be interdependent with payment system operators and third parties.

Risk profiles vary significantly based on the size and complexity of the financial institution's retail payment system products and services, IT infrastructure, and dependence on third parties. All financial institutions should maintain an effective internal control environment commensurate with the level of retail payment products and services offered. Effective internal controls should include financial, accounting, technical, procedural, and administrative controls necessary to minimize risks in the retail payment transaction, clearing, and settlement processes. These measures reduce operational and credit risks, ensure individual transactions are valid, and mitigate processing and other errors. Effective controls also ensure supporting IT and network infrastructure promote retail payment transaction integrity, confidentiality, and availability. Financial institutions engaging in retail payment system services should be aware of the risks inherent in the activity.

Financial institutions have always offered a variety of retail payment services; however, recent technological advances are expanding the opportunities for the development of innovative payment products and services. Financial institutions should recognize the reputation and strategic risk of newer products and services, which may lack consumer acceptance. Often, participants will also face uncertainty regarding how state and federal laws and regulations will apply to new payment systems. The ongoing shift from paper to electronic payments is increasing the participation of nonbanks in various payment functions, such as payment processing. Financial institutions should have a comprehensive and effective vendor and third-party service provider risk management and oversight program. [38]

Payment System Risk (PSR) Policy

Payment and securities settlement systems are critical components of the nation's financial system. The smooth functioning of these systems is vital to the financial stability of the U.S. economy. The Federal Reserve Board has developed the PSR policy to address risks that payments and securities settlement systems present to the financial system and to the Reserve Banks.

The Reserve Banks are exposed to credit risk when they process wholesale and retail payments for financial institutions holding reserve accounts, just as financial institutions assume credit risk when offering retail payments to their customers. Part of the Federal Reserve's PSR Policy seeks to control and reduce credit risk to the Reserve Banks by controlling financial institutions' use of Federal Reserve daylight overdrafts.

A daylight overdraft occurs when there are insufficient funds in a financial institution's Federal Reserve account to cover the institution's payment activity, such as outgoing Fedwire® funds transfers or ACH credit originations, as outgoing payments are posted during the day.

To control daylight overdrafts, the PSR policy establishes limits, or net debit caps, on the amount of Reserve Bank daylight credit that a depository institution may use during a single day and over a two-week reserve maintenance period. These limits are determined jointly through assessments by the depository institution and its Reserve Bank. The limits reflect the overall financial condition and operational capacity of each

institution using Reserve Bank payment services.

Financial institutions may be monitored on an ex post (i.e., end of day) or real-time basis. Under the Federal Reserve's ex post monitoring procedures, an institution with a daylight overdraft in excess of its maximum daylight overdraft capacity or net debit cap may be contacted by its Reserve Bank. The Reserve Bank may counsel the institution and discuss ways to reduce its excessive use of intraday credit. Each Reserve Bank retains the right to protect its risk exposure from individual institutions by unilaterally reducing net debit caps, imposing collateralization or clearing balance requirements, rejecting or delaying certain transactions, or, in extreme cases, taking the institution off-line or prohibiting it from using Fedwire. In addition, the Reserve Banks assess fees for daylight overdrafts above a certain deductible amount. [39] A Reserve Bank will monitor an institution's position in real time when the Reserve Bank believes that it faces excessive risk exposure, for example, from institutions with chronic overdrafts in excess of what the Reserve Bank determines is prudent. In addition, the Reserve Bank will reject or delay certain transactions that would exceed the institution's maximum daylight overdraft capacity or net debit caps, and take other prudential action, including requiring collateral.

Institutions that are monitored in real time must fund the total amount of their ACH credit originations in order for the transactions to be processed by the Reserve Bank, even if those transactions are processed one or two days before settlement. [40]

The financial institution's board of directors is responsible for PSR policy compliance and should ensure that management establishes sound internal operating practices, including compliance with applicable banking laws, and carefully manages retail payment system-related financial risks. At a minimum, a financial institution's board of directors and senior management should:

- Understand the financial institution's practices and controls regarding the risks of processing transactions for both its own account and the accounts of its customers and respondents;
- Manage its Federal Reserve account effectively and use daylight credit prudently in accordance with the PSR policy;
- Establish prudent limits on the daylight overdraft or net debit position in its Reserve Bank reserve account and any private-sector clearing and settlement system; and
- Review periodically the institution's daylight overdraft activity to ensure the institution operates within the established guidelines.

Strategic Risk

Strategic risk is associated with the financial institution's mission and future business plans. This risk category includes plans for entering new business lines, expanding existing services through mergers and acquisitions, and enhancing infrastructure (e.g., physical plant and equipment, IT, and networking). The variety of emerging technologies for retail payments demands integration of payment strategies into the financial institution's overall strategic planning processes. Financial institutions also compete increasingly with highly innovative nonbank entities to provide retail payment services.

This competition benefits the consumer through enhanced product offerings at a lower cost. Conversely, competition places additional pressure on financial institutions to protect profitability through the development of new products and services while managing additional marketing, research, and development costs.

Strategic plans that include significant market expansion or the addition of new products and services may expose financial institutions to increased risks. For example, expanding Internet banking services to include electronic bill presentment and payment services, expanding existing bankcard issuing programs, or entering the merchant bankcard processing business significantly increase the potential risk to the financial institution given the inherent risks associated with these services. Business plans for specific products and services should demonstrate that management has assessed the risks and documented the institution's program to mitigate them. Such plans should address the institution's capability to provide the service. Innovative products and services are emerging quickly and early stages of market introduction may expose financial institutions to undefined and unanticipated risks the need for an enterprise wide view of retail payment activities due to cross channel risk including fraud, money laundering, and IT security breaches. Business models for emerging products that are gaining acceptance abroad, particularly in Asia, may not be introduced as easily in the U.S. because of the differences in infrastructure and applications.

To mitigate strategic risk, management should have a strategic planning process [41] that addresses its retail payment business goals and objectives, including supporting IT components. Because financial institutions are increasingly reliant upon third-party service providers for retail payment system products and services, the strategic plan should address comprehensive vendor management.

Reputation Risk

Reputation risk occurs when negative publicity regarding an institution's business practices leads to a loss of revenue or litigation. For retail payment-related systems, reputation risk is linked to consumer expectations regarding the delivery of retail payment services, and the institution's ability to meet its regulatory and consumer protection obligations related to those services. An institution's reputation, particularly the trust afforded it by customers and counterparties can be irrevocably tarnished due to perceived or real breaches in its ability to conduct business securely and responsibly.

Financial institutions are responsible for risks associated with the activities of third-party service providers with which they contract. Deficiencies in security and privacy policies that result in the release of customer information by a service provider can damage the reputation of client financial institutions. Operational failures could significantly impact an institution's reputation if systems are disrupted for extended periods. Management oversight of third-party service providers is a critical component of reputation risk management.

Credit Risk

Credit risk arises when a party will not settle an obligation for full value. Each retail payment instrument has a specific settlement process that depends on the entities involved. Multiple financial institutions, third-party entities, as well as the payer and

payee are involved with creating, processing, and settling the transaction. If a financial institution uses a third-party service provider, the institution is responsible for the credit risk exposure for the services performed. Financial institutions should have procedures in place to manage the credit risk of third parties using the institution's accounts to settle transactions. [42]

Credit risk with retail payment systems is evident in ACH, merchant card, and remote deposit processes where the financial institution supplies funds on behalf of a merchant and provisional settlement does not occur for several days. Returns are another source of credit risk for all forms of retail payment systems. Checks and direct debit transfers can be returned by the payer's institution because of insufficient funds, a closed account, a stop payment order, forgery, fraud, or other payment irregularity. The return timeframes vary for different payment instruments. For an ACH debit, the ODFI grants funds availability to the originator on settlement day. The credit exposure exists until the RDFI can no longer return the ACH debit. If not properly authorized, the return time frame for consumer debits under NACHA rules extends to 60 days from the settlement date.

Financial institutions that accept large volumes of retail payments from merchants should understand the nature and degree of credit risk from those relationships. Financial institutions should manage those relationships in the same manner as any credit, subjecting the customers to credit administration processes for due diligence and ongoing monitoring. The risk in large volume relationships, and the institution's legal lending limit and capital position should be recognized in establishing exposure limits for each customer. Financial institutions may mitigate credit risk by requiring pre-funding for credit originators and adequate risk- based reserves for debit originators.

For the ACH system, NACHA rules require each ODFI to conduct appropriate creditworthiness monitoring, establish exposure limits, and periodically review the limits applicable to specific originating customers. Both ODFIs and RDFIs are exposed to credit risk. However, an RDFI's credit risk is minimal because it has the right to return items it is unable to post to customers' transaction accounts within NACHA guidelines and timeframes. ODFIs are ultimately responsible for all transactions entering the payment system regardless if the transaction is a credit or a debit. ODFIs that generate credits have a typical credit exposure of three days, which represents the gap between the submission of the ACH credit file and the funding of the file by the file originator. Such credit risk may be mitigated by requiring pre-funding of the credit file. ODFIs that generate debits have a credit exposure of 60 days due to the potential for returns.

Bankcards have specific procedures for chargebacks, which are amounts disputed by the cardholder and "charged back" or reversed out of the merchant's account. The acquiring financial institution relies on the creditworthiness of the merchant, but if the merchant declares bankruptcy, commits fraud, or is otherwise unable to pay its chargebacks, the acquiring financial institution must pay the issuing financial institution.

The settlement of retail payment transactions (i.e., the transfer of funds between the parties) discharges the payment obligation. The risk that settlement of retail payment transactions will not take place as expected can result in both credit and liquidity risks. Financial institutions should understand and manage credit and liquidity risks related to the settlement of retail payments. This should include preparing for potential credit and liquidity issues resulting from incomplete settlement or operational problems.

Settlement lags occur when financial institutions, due to failure or the inability to fund their obligations, do not settle their obligations when due. Settlement lags result in credit risk until final settlement occurs. Any payment activity undertaken on the basis of

"unsettled" payment messages remains conditional, resulting in risk. Settlement lags may also result in liquidity risk. Until settlement is completed, a financial institution is not certain what funds it will receive through the payment system. As a result, it may not be sure whether its liquidity is adequate. If an institution overestimates the funds it will receive when settlement takes place, it may face a shortfall. If the shortfall occurs close to the end of the day, an institution could have significant difficulty finding an alternate liquidity source.

Financial institutions often allow their corporate customers to incur intraday or "daylight" overdrafts. An institution engaging in this practice is extending credit to its customer. In most cases, the overdraft is eliminated with incoming funds transfers from other institutions (or outgoing securities transfers against payment) by the end of the business day. Daylight overdrafts constitute an extension of credit, no matter how long they remain unpaid. An institution's credit policies should include provisions for approving and monitoring daylight overdraft lines to customers.

Liquidity Risk

Liquidity risk is the current and potential risk to earnings or capital arising from a financial institution's inability to meet its obligations when they come due without incurring unacceptable losses. Liquidity risk related to payment systems is the risk that the financial institution cannot settle an obligation for full value when it is due but rather at some unspecified time in the future. Liquidity problems can result in opportunity costs, defaults on other obligations, and costs associated with obtaining the funds from an alternative source for possibly extended periods of time. In addition, operational failures may also negatively affect liquidity if payments do not settle within an expected time period.

Legal (Compliance) Risk

Legal risk arises from failure to comply with statutory or regulatory obligations. It can result from a financial institution's failure to comply with the bylaws and contractual agreements established with the bankcard networks, clearing houses, and other counterparties with which it participates in processing, clearing, and settling retail payment transactions. Legal risk also arises if the rights and obligations of parties involved in a payment are subject to considerable uncertainty; for example, if the rights of the parties are not clear when a payment participant declares bankruptcy or if a court interprets an applicable law in an unexpected way. In addition, legal risk can occur when customer agreements or contracts do not clearly establish the roles, responsibilities, governing regulations or guidelines, and dispute resolution processes, particularly with regard to RDC. Legal disputes that delay or prevent the resolution of payment settlement can cause credit, liquidity, or reputation risks at individual institutions. Though unlikely, these disputes also can cause potential systemic risk to the payments system. Legal risk also arises from noncompliance with existing consumer protection statutes, regulations, and case law governing retail payment transactions (e.g., Gramm-Leach- Bliley Act or GLBA, Truth in Lending Act, Regulation CC, and Regulation E). Customer retail payment transaction records and corresponding account information are subject to the GLBA 501 (b) provisions, and financial institutions must establish effective safeguards for protecting their customer information. The bylaws and agreements between clearing house participants and bankcard companies also include specific responsibilities and liabilities.

Financial institutions and third-party service providers that do not comply with the appropriate bylaws and agreements of bankcard companies and clearing houses can be fined or lose their memberships. Thus, financial institutions should assess the risks of accepting such bylaws and agreements in their strategic planning process for new payment offerings. Given the rapidly changing landscape for electronic funds processing, it is paramount for a financial institution to pay close attention to changing legal and regulatory requirements, as well as new network rules that might create unexpected liability for the institution. As financial institutions enter into merchant card, ACH, and remote check processing arrangements with third-party service providers and originators, the institution should ensure that all such arrangements are governed by clearly written contracts which define outsourced responsibilities and liabilities. Financial institutions should carefully review contracts with third parties for outsourced services to ensure that they are not assuming the full risk of loss from failure of third parties to fulfill their contractual responsibilities. Contractual terms may further define responsibilities within the legal framework; and contracts between financial institutions, customers, and third-party service providers may further integrate risk-sharing responsibilities applicable to payments made through a specific clearing or settlement arrangement. In some cases, emerging product development may have insufficient case law to support a completely accurate analysis of the potential risk horizon. The convergence and interoperability of older, more traditional payment methods with newer technologically supported payments may create questions regarding the applicability of law and regulations governing both consumer protection and retail payment transactions. In most cases, older payment technologies for more mature retail payments (checks and credit cards) may co-exist with newer payments technologies requiring financial institutions to maintain several systems. The emergence of hybrid systems that incorporate older technologies with newer payments will require heightened review to mitigate and control legal risks. Hybrid systems and new payment technologies also increase the risk of money laundering as a result of increased volumes, transaction speed, and anonymity. Financial institutions should ensure that due diligence for new payment products or services fully evaluates the applicability of laws and regulations, regulatory guidance, and payment association rules from organizations such as NACHA, Visa, and MasterCard. Recent developments in payments over the ACH system raise legal questions regarding whether payments should be characterized as checks or electronic fund transfers. The same questions arise with respect to RDC and electronically created payment orders. As stated previously, in 2006 the Federal Reserve amended Regulation CC, shifting the liability for losses attributable to unauthorized RCCs to the depository financial institution where the check is first cashed or deposited. The liability creates an economic incentive for depository institutions to perform due diligence on the customers and RCCs. These amendments do not affect the rights of checking account customers, as they are not liable for unauthorized checks drawn on their accounts. The fact that a payment may take several different forms, both paper and electronic, during the course of processing and settlement, creates additional complexity. A payment transaction may be covered by check law, Regulation E, association or clearing house rules, or private agreement, depending on what form the payment takes. Financial institutions should understand the laws and rules that apply to payments they handle and understand the associated legal risks and liabilities they take on with respect to those payments.Bank Secrecy Act (BSA) The BSA requires financial institutions to have BSA/Anti-money laundering (AML) compliance programs and appropriate policies, procedures, and processes in place to monitor, identify unusual activity, and report suspicious activity. As such, all retail payment systems should be reviewed in terms of BSA/AML compliance requirements. The FFIEC BSA/AML Examination Manual includes examiner guidance and expectations for ACH and other payment systems that may require the collaboration of Operational, IT, and BSA examiners. This Booklet does not seek to replicate the guidance and expectations, however, and only a brief summary of this compliance risk is

offered.44 Office of Foreign Assets Control (OFAC) OFAC administers and enforces economic sanction programs directed against countries and groups of individuals such as terrorists and narcotics traffickers. All U.S. persons and incorporated entities involved in a payment transaction (i.e., all U.S. citizens and permanent resident aliens, wherever located; all persons and entities within the U.S.; and all U.S. incorporated entities and their foreign branches) are subject to OFAC regulations.45 For domestic ACH transactions, the ODFI is responsible for verifying that the originator of the ACH instruction is not a blocked party and for making a good faith effort to determine that the originator is not transmitting blocked funds. The contract between the ODFI and its customer should clearly define the customers' responsibilities to verify that the originator is not a blocked party and to make a good faith effort to determine the originator is not transmitting blocked funds. For high risk originating customers, the ODFI may wish to request that originating customers provide an independent validation of its controls for preventing transmission of funds to blocked parties. The RDFI is responsible for verifying that the receiver of the ACH funds is not a blocked party. For domestic ACH transactions, if ODFIs receive batched transactions from their customers that do not include international ACH transactions, they are not responsible for un-batching transactions and ensuring that they do not process transactions in violation of OFAC's regulations. If the ODFI un-batches the transactions received from its customers, or receives batched international ACH transactions, it is responsible for screening as though it had made the initial batching. For outbound international ACH transactions, on the other hand, the ODFI cannot rely upon the RDFI for OFAC screening. For inbound international ACH transactions, the RDFI is responsible for compliance with OFAC regulations.

Operational Risk

Operational risk is the risk of loss resulting from inadequate or failed internal processes, people and systems, or external events. Operational risk can arise from a technology failure, human or technical errors in financial models and reporting, or other internal control system deficiencies. In the case of RDC, operational risk (i.e., image/data quality, business continuity, information security, etc.) increases when deposit processing occurs at the customer location which is outside of the financial institution's direct control. As a result, the financial institution could experience delays or disruptions in processing, clearing, and settling retail payment transactions that could lead to credit and liquidity problems at other financial institutions.

Operational risk can also arise from fraud perpetrated by employees or by external sources. A financial institution is exposed to operational risk from fraud when a wrongful or criminal deception can lead to a financial loss for one of the parties involved. While fraud risk in traditional ACH activity is low, new ACH products and services, such as one-time ACH debits from Internet-based and telemarketing merchants (WEB and TEL) pose considerable fraud potential. With traditional ACH activity, financial institutions have employed strong front-end fraud controls for recurring debits they originate. These controls are typically not present with WEB and TEL transactions. The continuing growth of check-to-ACH conversion, check truncation, and the growing use of RCCs, RDC, and electronically created payment orders present new forms of fraud risks. In these situations, liability typically rests with the financial institution where the check is first deposited or the ACH item is originated. In the case of electronically created payment orders, liability rests with the financial institution that sends the file to the Reserve Bank or other correspondent. As operational processes continue to change, financial institutions will need to enhance their internal controls, as described below, to mitigate

operational risk. Existing control mechanisms may not be as effective as necessary.

Newer retail payment mechanisms, particularly using the Internet, also subject customers and financial institutions to fraud risk exposure. All of these highly automated processes typically reflect a reengineering of the existing check processes, and the existing fraud controls may not be adequate. The creation of fraudulent electronic transactions could lead to financial losses if fraudulent balances are successfully exchanged for a readily transferable form of funds, such as currency.

Operational risk controls should include sound information systems, and procedural, administrative and legal measures to prevent or limit financial loss. System measures include monetary and time limits (per transaction, per payment instrument, per client), personal authentication, and encryption techniques to ensure the authenticity and integrity of the payer and transaction information. Additional controls include the use of certified, tamper-resistant equipment (e.g., EFT/POS terminals), logical access controls to verify transactions, online verification of account balances, logging of all transactions and attempts to make a transaction, and the use of serial numbers and check digits.

Financial institutions can create a fraud detection control through a due diligence program for new account acceptance coupled with ongoing, automated monitoring of deposit account transactions. Account monitoring should be facilitated through the use of caps, limits, and triggers to measure activity on an intraday basis. Financial institutions use a variety of automated databases, such as credit bureaus, to review new accounts prior to or soon after opening the accounts. Institutions also use a number of vendor-supported automated algorithms to review deposit account transactions for unusual activity related to kiting or other fraud.

Other procedural measures for reducing fraud include: closely monitoring return rates for all customers, appropriate dual custody and separation of duties for critical payment transaction processing and accounting tasks, payment data verification, clear error processing and escalation procedures, and confidential and tamper-resistant mailing procedures for bankcards and other sensitive material. Account reconcilement processes are vital to early detection of errors and fraud. Administrative measures should include IT audit coverage of operational controls, legal controls (including regulatory compliance and agreements), and personnel issues associated with staffing and training.

In the event of an unauthorized use of a payment card, the cardholder's liability is limited to a specified amount if he or she notifies the card issuer of the theft or loss within a set time limit. To limit their own losses from POS card fraud, the bankcard companies require vendors to match the cardholder's signature on the card with the signature on the payment voucher at the POS. The bankcard companies have also introduced extensive monitoring and reporting controls to limit fraudulent activity.

In a broader view of operational risk management, financial institutions should employ vendor management programs that provide for due diligence of new service providers as well as ongoing monitoring of existing vendors. An effective vendor management program will focus on data security and business continuity.

In addition, a more effective approach to mitigate fraud risk may be to view this risk potential across channels. This requires an enterprise view of the range of retail payments activities. Those payments that use multiple payment channels for processing and clearing are subject to an increased level of fraud risk because traditional fraud detection and prevention measures are designed for single channels. Fraud is more likely to migrate to those channels where fraud detection and prevention measures are

less developed.

Mitigation of Operational Risk

Financial institutions should adopt measures that limit operational risks arising from the processing, clearing, and settlement of retail payments. Financial institutions and technology service providers participating in clearing and settlement arrangements for retail payments should ensure operational reliability for timely completion of daily processing through adequate information systems, internal controls, backup facilities, reliable technology, and adequate staff training and support. Furthermore, these organizations should adopt business continuity plans to minimize and manage the effects of interruptions. Risk analysis should identify confidential assets, critical operations, and potential threats. It should also define safeguards and countermeasures to provide appropriate protection.

Risk from fraud or error from customers that generate high volumes of RDCs, electronically created payment orders, or RCCs can be managed more effectively with the use of activity and fraud monitoring tools for those customers. Financial institutions that originate large volumes of ACH transactions directly or through third-party service providers should also consider these tools as part of their due diligence. Fraud databases and fraud analysis tools can assist financial institutions in detecting and controlling potential fraud risk. Some bankcard associations and Internet banking applications use neural network technologies or behavioral fraud analysis. These technologies utilize specialized software and hardware designed to identify patterns of behavior that enable financial institutions to identify suspicious transactions or spending. The bankcard companies have also developed numerous fraud detection and avoidance systems that member financial institutions can use to reduce losses as a result of fraudulent bankcard use. The growth of e-commerce has led many financial institutions and service providers to develop additional databases that provide early identification of potential fraud.

Identifying, evaluating, and addressing potential legal and compliance risks associated with new payment systems providers can also help mitigate operational risk. For example, a thorough legal review process can ensure that there are clearly defined roles and responsibilities for the financial institution, its service providers, and its customers. Financial institutions should also comply with the regulations and consumer compliance mandates that apply to retail payment services (e.g., Regulation E).

Financial institutions also should have appropriate risk control functions such as audit, information security, vendor management, and business continuity, as discussed in the following sections.

Audit

Action Summary

The board of directors should ensure that an effective internal audit function for the financial institution's payment systems is in place. The audit program should test the quality of retail payment systems internal controls and compliance with laws, regulations, management policies, procedures, and limits. Audit coverage should be

risk-focused and should cover all retail payment systems including third party relationships. Special attention should be given to new retail payment technologies and products.

An effective audit function should include internal and external audit coverage, tailored to the complexity of the financial institution, and based upon an accurate, enterprise-wide assessment of the institution's risk profile. Due to the potentially large transaction volumes and associated dollar value when initiating payments, internal audit coverage is critical for an effective oversight of the financial institution's retail payment systems. Auditors should perform an evaluation of the financial institution's retail payment system business lines on the basis of overall risk to the financial institution. Based on this evaluation, they should develop an appropriate schedule of audits. The audit coverage should be sufficient to validate the internal control environment surrounding the processing, clearance, and settlement of retail payment transactions. Auditors should review accounting controls and assess the effectiveness of transaction processing, clearance, and settlement processing procedures.

The board of directors should ensure the operational and IT audit program tests retail payment system internal controls, management policies, and procedures. IT audit coverage should include the design and implementation of retail payment products, and the supporting IT environment encompassing internal data centers, contingency sites, and network infrastructure. IT audit coverage should verify the adequacy of internal controls in applicable business lines responsible for managing day-to-day retail payment system services. Internal audit should assess the comprehensiveness of the institution's vendor management program to ensure the institution is appropriately managing vendor risk. [43] Internal audit should also evaluate payment systems when conducting BSA audits.

Information Security

Action Summary

Financial institutions should implement the appropriate physical and logical security controls to ensure retail payment system transactions are processed, cleared, and settled in an accurate, timely, and reliable manner. Security risk assessments should consider physical and logical security controls for the origination, approval, transmission, and storage of retail payment system transactions. Risk assessments should include service providers, third-party originators, and external networks that process, store, or transport customer data. Physical controls should limit access to only those staff assigned responsibility for supporting the operations and business line centers that process retail payment and accounting transactions. Physical controls should also provide for the ability to monitor and document access to these facilities. Logical controls should include identifying and authenticating retail payment system customers to help ensure the integrity of the payments. Particular attention to data security is required for emerging technologies.

Financial institutions should implement the appropriate physical and logical security controls to ensure retail payment system transactions are processed, cleared, and settled in an accurate, timely, and reliable manner. Retail payment systems contain confidential customer information subject to GLBA section 501(b) security guidelines. Payments data may also be subject to the requirements of the Payment Card Industry Data Security Standard (PCI DSS). [44] The board and management are responsible for protecting the confidentiality, integrity, and availability of these systems and data. The privacy risk combined with the funds transfer capability should cause these systems to rank high in all institutions' information security risk assessments. The risk assessments should consider physical and logical security controls for the origination, approval, transmission, and storage of retail payment system transactions.

Physical controls should limit access to sensitive areas to staff assigned responsibility for supporting the operations and business line centers that process retail payment and accounting transactions. Physical controls should also provide for monitoring and documenting access to these facilities.

Management should assign appropriate logical access to staff responsible for retail payment-related services and should base access rights on the need to separate the duties of personnel responsible for originating, approving, and processing the transactions. Appropriate identification and authentication techniques include requiring unique authenticators for each staff member with strong password requirements.

Logical access controls should permit access on a need-to-know basis and should assign access to retail payment applications and data based on functional job duties and requirements. Logical access controls should also protect network access. An institution's risk assessment should require protection of retail payment systems from unauthorized access through appropriate access controls, network and host configuration, operation, firewalls, and intrusion detection and monitoring. The risk assessment should also review the security of all third-party service providers. Some institutions accomplish this by isolating all payment-related applications and systems from other production applications.

A critical element in ensuring retail payment systems integrity is the appropriate identification and authentication of retail payment system customers. Transaction authorization (e.g., the approval of a funds transfer or guarantee of funds) is an essential precondition leading to the interbank transfer of funds. Financial institutions should establish an adequate internal control environment for the issuance of bankcards and related PIN. These controls can minimize processing errors and fraud and protect the confidentiality of customer and institution information.

The use of newer and emerging technologies presents new security challenges. As new retail payment products and services are developed, it may become necessary to modify methods for customer identification and authentication to ensure their effectiveness.

Many electronic banking applications use Internet-based, open network standards and rely on commonly accepted technologies to secure transmissions (e.g., secure socket layer [SSL] or other virtual private network [VPN]). The institution should establish a secure session before consumers can submit their personal banking information, and

should maintain the secure session until the time of final data transmission.

Retail payment systems should incorporate sufficient security procedures and controls to verify the integrity of the data, the confidentiality of the transmission, and the authenticity of the communication partners and data sources. The selection and use of authentication technologies and methods should depend upon the results of a financial institution's risk assessment process. Where risk assessments indicate that the use of single-factor authentication is inadequate, financial institutions should implement multifactor authentication, layered security, or other controls reasonably calculated to mitigate those risks. Single factor authentication alone is inadequate for high-risk transactions involving access to customer information or the movement of funds to other parties. Using digital certificates, leveraging the public key infrastructure (PKI), employing biometrics and card or token-based techniques can provide cost-effective solutions for augmenting traditional technical controls. [45]

Institutions that participate in payment card systems should develop processes to ensure compliance with the PCI DSS. This standard is discussed further in the "Merchant Acquiring" section.

Institutions should have a response program in place that addresses security breaches, including incidents with their third-party servicers. The program should include the investigation, customer notification, if applicable, and reporting processes for regulatory and law enforcement agencies.

Business Continuity Planning

Action Summary

Financial institutions and their TSPs should develop, implement, and test appropriate disaster recovery and business continuity plans capable of maintaining acceptable retail payment-related customer service levels. For financial institutions and service providers with complex retail payment operations, business continuity plans should enable restoration of service within timeframes that are reasonable for internal business units as well as other dependent financial institutions and counterparties.

Effective business continuity planning is an important component in managing operational risk. Financial institutions and their TSPs should develop, implement, and test appropriate disaster recovery and business continuity plans capable of maintaining acceptable retail payment-related customer service levels. Business continuity plans should be based on business impact analyses and the relative importance of retail payment system products and services to the financial institution. [46]

For financial institutions offering basic retail payment products and services (e.g., bankcard issuance, check item processing, branch ATM access, Internet banking services), business continuity plans should include appropriate recovery targets for each retail product. The recovery targets should consider the reliance on any third-party servicer in meeting their objectives. Vendor management programs should include provisions for the disruption and restoration of service at service providers, including the consideration of service provider test plans.

For financial institutions and service providers with complex retail payment operations, business continuity plans should enable restoration of service within timeframes that are reasonable for internal business units, other dependent financial institutions, and counterparties. Financial institutions providing significant card issuing, merchant processing, EFT/POS, ACH, and retail payment-related Internet banking services should also test these plans periodically with customer financial institutions and counterparties to ensure plans are sufficient.

Vendor and Third-Party Management

Action Summary

Financial institutions should establish and maintain effective vendor and third-party management programs because of the increasing reliance on nonbank providers. Financial institutions must understand the complex nature of arrangements with outside parties and ensure adequate due diligence for the engagement of the relationships and ongoing monitoring.

Some financial institutions rely on third-party service providers and other financial institutions to provide retail payment system products and services to their customers. Many retail payment services are directly related to core processing financial institution operations (e.g., accessing demand deposit accounts through the use of financial institution-issued bankcards) and may be run in-house through the use of purchased turnkey systems. However, financial institutions outsource many retail payment-related services to third parties, including foreign-based, either to enhance the services performed in-house or to offer new retail payment services that are otherwise not cost effective.

To ensure retail payment operations are conducted appropriately, financial institutions should have comprehensive contract provisions and adequate due diligence processes. They should also monitor service providers for compliance with contracts and service level agreements. Effective monitoring should include the review of select retail payment transaction items to ensure they are accurate and processed timely. The integrity and accuracy of retail payment transactions posted to customer accounts depend on the use of proper control procedures throughout all phases of processing, including outsourced functions.

Regardless of whether the financial institution's control procedures are manual or automated, internal controls should address the areas of transaction initiation, data entry, computer processing, and distribution of output reports. These control considerations apply to processing checks, including through RDC, as well as electronically created payment orders, electronic bankcard, debit card, and ACH transactions. Financial institutions must also maintain effective control over service provider access to customer and financial institution information consistent with GLBA section 501(b). Contractual

provisions should define the terms of acceptable access and potential liabilities in the event of fraud or processing errors. [47]

Retail Payment Instrument Specific Risk Management Controls

Action Summary

Specific retail payment instruments introduce risks that require effective internal controls and adherence to the relevant clearing house, association, interchange, and regulatory requirements. Financial institutions should address these risks in their information security and business continuity planning programs

Checks

Financial institutions manage the risk exposure to check payment processing by establishing appropriate account opening and monitoring controls. Account opening controls that incorporate information from credit bureau services may mitigate credit risk exposure to criminals and to customers with a history of financial problems. Such screening is also the basis for customer verification in support of BSA/AML compliance and for qualifying customers for RDC. Institutions should perform a credit assessment of those customers for whom they collect large dollar volumes of checks.

Financial institutions use a variety of monitoring tools during check processing as a means of identifying potential fraudulent activity or for early detection of kiting. These automated tools are typically available from major vendors. Institutions should monitor the payment activity of their customers and take appropriate action when credit limits are exceeded or when their business practices may indicate possible fraud or money laundering activity. Institutions that offer commercial customers services for RDC should make such arrangements under contracts that clearly state the liability of the commercial customer in the event of a dispute over the imaged checks.

Regulation CC requires that when a paying financial institution decides to return a check of $2,500 or more, it must provide a notice of nonpayment to the depository financial institution, in which the check was deposited, to mitigate the depositary institution's financial loss in case the customer tries to withdraw funds represented by the returned check. Regulation CC also requires a check to be returned to the depository financial institution expeditiously, regardless of the amount. A paying bank returns a check expeditiously if it returns the check to the depositary bank within two business days of presentment (for local checks) or four business days (for nonlocal checks). Alternatively, a bank returns a check expeditiously if it sends the check in the same manner as it (or a similarly situated bank) would have sent the check for forward collection.

Using ECP for payment can reduce risks to depository financial institutions because it permits them to deliver check data to paying financial institutions more quickly than by presenting paper checks. The shorter delivery time permits paying financial institutions to (1) identify checks that cannot be paid and (2) notify the depository financial institution

about those returned checks using an electronic return notice and up to one day earlier than would occur with the physical exchange of paper checks.

Check truncation (the conversion of MICR information to electronic form), on the other hand, introduces the risk of unauthorized changes to converted check information in transmission or in storage. As with RDC, this risk may increase when truncation occurs at the customer location. Financial institutions should develop and implement appropriate information processing safeguards to mitigate this risk. These safeguards should include logical access controls and separation of duties to minimize potential tampering with electronically converted check information and images during processing, and to ensure the MICR and check image databases are protected from unauthorized access. Check truncation also introduces the risk that a customer's account may be debited twice for the same check. This happens either when the MICR data is read, the account is debited, and the check is accidentally sent to the proof/sorter where it is read again and the account is debited a second time or when an electronic check file is inadvertently duplicated. Financial institutions should develop preventive controls to avert checks from being read twice or electronic check files from being duplicated or processed twice, and they should have detective controls to determine whether debits arise from the same check. These controls should also be applied to processes where checks are converted to ACH debits.

Check fraud is a significant factor in losses reported by financial institutions. The leading form of check fraud is check kiting; that is, presenting checks to two or more financial institutions for the purpose of fraudulently obtaining interest-free unauthorized loans. Other types of check fraud include forged, altered, and counterfeit checks. "Positive pay" is a technique that can reduce check fraud by requesting businesses to send electronic files of information to the financial institution on all checks the business has issued. The financial institution compares this information against electronic information regarding checks presented for payment. If a check presented for payment is not included in the positive-pay information, the institution requests the corporation to make a pay/no pay decision.

ACH

ACH operations pose a variety of risks including credit, liquidity, and operational. NACHA and the two national ACH operators (the Reserve Banks and EPN) have clear expectations that financial institutions will manage these risks, particularly when the institutions engage in riskier ACH activities. In recent years, the ACH operators have begun to offer a variety of risk management tools to help control ACH risks. Financial institutions should employ those tools that are commensurate with the risks taken.

The risk of fraud can be mitigated through proper due diligence for all originating customers and strict adherence to ACH and credit policies. Additional mitigation can be achieved by avoiding high risk businesses and customers. Limits should be appropriate for the risks of each customer and the use of pre-funding arrangements or reserves can be effective in controlling losses. Management should review monitoring reports offered by the ACH operators that can assist in early detection of unauthorized ACH transactions.

For ACH credit entries, a financial institution that serves as the ODFI incurs credit risk upon initiating the entries until its customer funds the account. The ODFI is responsible for settling payments originated using its routing number even if the transactions are outsourced to third-party service providers. The RDFI incurs credit risk when it grants

funds availability to its customer prior to the final settlement of the credit entry. For ACH debit entries, the ODFI incurs credit risk from the time it grants funds availability to the originator (usually on the settlement day) until the ACH debit can no longer be returned by the RDFI. If the transaction is properly authorized, returns must be made no later than the second banking day following settlement. If not authorized properly, the financial institution exposure can be up to 60 days from when it sends a periodic statement to the consumer. An ODFI will normally charge back a returned ACH debit to the originator. However, the ODFI may suffer a loss if the originating account has insufficient funds, is closed, or is frozen because of bankruptcy or other legal action.

To manage its credit exposures, an ODFI should establish policies, procedures, and limits that acknowledge the risks certain businesses and customers bring to an ACH operation. Higher risk businesses include gambling and adult entertainment firms. The financial institution's policies should clearly state the types of businesses and customers that are acceptable and should treat all ACH customers as unsecured borrowers that are subject to the institution's standard credit review and approval process. An ODFI should conduct thorough due diligence of its originating customers, including understanding the nature of their businesses and financial condition. For certain customers, pre-funding or reserve arrangements may be necessary to control the risk. On an ongoing basis, an ODFI (and its service providers) should monitor the creditworthiness of its customers, and establish and periodically review ACH exposure limits for them. In addition, an ODFI should implement procedures to monitor ACH entries relative to the originator's exposure limit across multiple settlement dates. Breaches in limits should be reported to the appropriate levels of management. An ODFI should monitor and research frequently the returns, particularly unauthorized returns. The Federal Reserve and EPN can provide such reports to ODFIs.

An RDFI should establish prudent overdraft and funds availability policies and practices to mitigate its credit exposures. Credit risk, with respect to a debit entry, arises if the RDFI allows the debit to overdraw its customer's account. When a financial institution fails to comply with the NACHA rules, it exposes itself to contractual liability and fines. In addition, Regulation E applies to electronic fund transfers, including ACH transactions. The notice, authorization, error resolution, and timing requirements of Regulation E are of particular importance. Noncompliance with Regulation E exposes a financial institution to litigation and civil money penalties. Financial institutions should also monitor their compliance with applicable BSA and OFAC requirements concerning unusual transactions and transactions involving blocked parties.

Financial institutions should understand the impact that ACH transaction risk has on their liquidity. For example, an ODFI may not be able to settle (collect) an ACH debit, or an RDFI may not be able to settle an ACH credit because of fraud, service disruption, or the default of an ACH Network participant. This could impair the financial institution's ability to meet its obligations and result in losses. Financial institutions should consider the volume of their uncollected ACH transactions as part of their liquidity risk management practices. For certain customers, pre-funding arrangements may be used to reduce liquidity risk.

Given the highly automated nature of ACH activities, operational risks should be managed closely. Clear policies and procedures should establish the proper control environment. Exceptions and operational problems, including processing delays and customer complaints, should be monitored in a timely manner. Management and staff should be familiar with NACHA rules and the requirements of the Reserve Banks and EPN. Well conceived and tested contingency plans are vital given the time sensitive nature of ACH transactions. Higher expectations for BSA compliance require additional

attention from management. Audits should be performed on a frequent basis by qualified auditors.

Third-Party ACH Processing

While a financial institution's responsibilities do not change with the use of a technology service provider for ACH processing, its risk exposure may increase as a result of the servicer's direct access to an ACH operator. A TSP may transmit ACH transactions directly to an ACH operator using the ODFI routing number. However, it is the ODFI that warrants the validity of each entry transmitted by the service provider, including the basic requirement that a receiver has authorized all entries. To reduce risk to all parties, the financial institution should establish controls over TSP operations, and the ODFI should maintain control over its settlement accounts. [48]

Although the federal regulators do not enforce the NACHA rules, a financial institution subject to them should have appropriate risk-management and control processes to ensure compliance with these rules. For example, NACHA requires TSPs performing ACH processing functions on behalf of an ODFI or RDFI to conduct an annual compliance audit covering the requirements of their rules. The financial institution should review and assess all audits of its service provider's internal controls. NACHA rules also require the ODFI to have contractual agreements with third-party senders specifying that the third-party sender is in compliance with NACHA rules and applicable laws and regulations. NACHA rules further require the ODFI to have an agreement with a TSP that has direct access to an ACH operator. NACHA specifies that the agreement sets out the rights and responsibilities of all parties, including:

- A requirement that the third-party service provider obtain the prior approval of the ODFI before originating ACH transactions for originators under the ODFI routing number. ODFI approval of each originator should be contingent upon the creditworthiness of the originator and the execution of an originator and ODFI agreement.
- ODFI dollar limits for files that a TSP deposits with the ACH operator. The service provider should notify the ODFI of any file exceeding established dollar limits before depositing the file at the ACH operator so that the ODFI can either approve it as an exception or hold it until the next business day.
- A provision that restricts the TSP's ability to initiate corrections to files already transmitted to the ACH operator. The ODFI should restrict correction capability. If the TSP has the ability to make file corrections, the ODFI should authorize and approve any changes to the file totals before the ACH operator releases the file for processing. [49]
- A requirement that a third-party sender who enters into an agreement with an ODFI establish the identity of each originator using commercially reasonable methods, warrant that the originators will assume their responsibilities under NACHA rules, and warrant that it will assume the liabilities of the ODFI. [50] The lack of a direct relationship between the ODFI and the originator poses a risk to the ODFI. The ODFI should conduct proper due diligence, establish exposure limits, and employ other monitoring procedures to ensure that the business practices of the third- party sender and its merchant clients do not create an undue risk to the ODFI. The ODFI

should be able to substantiate that the third-party sender has sufficient creditworthiness to back the warranties it makes relative to the risk, nature, and volume of ACH transactions; the underlying originators; and the exposure duration.

NACHA also requires participating financial institutions to conduct annual audits of their ACH operations to assess compliance with NACHA rules. These audits can provide examiners with insights into the quality of ACH operations.

Risk Considerations for Business Banking EFT Payments

Financial institutions that offer corporate customers access to Web-based business banking applications to facilitate the direct origination of payments (e.g., ACH credits/ debits, wire transfers, etc.) create special risk considerations for the financial institution and its corporate customers. These applications offer corporate customers an efficient way to conduct treasury management activities such as invoice payments and funds transfers. However, these features also increase the velocity in which errors and fraud can subject businesses or the bank to loss and can be the target of malicious software designed to circumvent online authentication methods to obtain credentials that can be used to initiate fraudulent payments.

Ongoing education of corporate customers remains one of the best ways financial institutions can mitigate the risks associated with online business banking applications. This is especially the case for some small businesses and community-based corporate entities (e.g., churches, schools, etc.) where the awareness of payments fraud techniques may be limited and the impact of a fraud can be significant. In addition to providing a secure environment for corporate payments (e.g., strong encryption, transaction risk profiling, etc.), financial institutions can help mitigate corporate payments risk by ensuring their corporate customers understand the importance of good business practices such as payment origination dual controls, daily account reconciliation, and other measures to protect the integrity of the corporate customers computer systems (e.g., virus protection, operating system upgrades, etc.).

Credit Cards

Credit and fraud losses are two of the most significant credit card-related risks to a financial institution. Credit losses due to contractual delinquency and bankruptcy account for the majority of credit card charge-offs. Fraud includes unauthorized use of lost or stolen cards, fraudulent applications, counterfeit or altered cards, and the unauthorized use of a cardholder's credit card number for card-not-present transactions.

Consumer compliance regulations (Regulation Z and Regulation E) and association operating rules (Visa and MasterCard) provide significant consumer protection for fraudulent transactions. According to Regulation E, if cardholders report timely the loss of their credit cards, they are responsible for no more than $50 of the charges resulting from fraud. Regulation Z provides additional billing error resolution procedures. Visa, MasterCard, Discover, and American Express have zero liability programs, which indemnify card holders for all fraudulent losses in many circumstances. The issuing financial institution or the merchant pays the costs of any fraud involving credit cards. At a minimum, the merchant should obtain an authorization, a cardholder's signature, or an electronic imprint of the card (electronic information on the card) at the POS. The merchant is required by the card companies to cover fraudulent transactions through the

chargeback process if it does not follow the minimum procedures. This has become a significant issue for many online retailers processing card-not-present transactions. The major bankcard companies; however, have introduced services to reduce the liability of the merchants. Under one initiative, issuers will assume losses for fraudulent transactions if the payment was authorized using the bankcard company's authentication procedures.

A control method financial institutions use to reduce risk is the authorization process to approve the credit transaction. For example, when the merchant swipes the bankcard, the issuer can deny authorization of the transaction if the consumer is over his or her credit limit, is delinquent, or if the card has been reported as stolen. Financial institutions can also employ the address verification service (AVS) to verify a cardholder's billing address and other pertinent information. AVS is used for mail, telephone, and Internet transactions.

Employing the appropriate underwriting, account management, monitoring, and collection practices can mitigate credit risk. By setting standards that reduce the probability of delinquency and fraud, financial institutions can more effectively control credit losses.

Debit/ATM Cards

A significant risk with PIN or signature-based debit or ATM cards is that unauthorized individuals will obtain them and make fraudulent transactions. Financial institutions and their technology service providers should mitigate these risks by executing financial institution-merchant and financial institution-customer contracts that delineate each party's liabilities and responsibilities. Institutions should also establish adequate physical safeguards including the installation of surveillance cameras and access/entry control devices. State and federal laws, particularly Regulation E, protect consumers by limiting their liability if they give notice of lost or stolen cards, or of unauthorized EFTs within a specified period.

ATM stand-in arrangements, which enable EFT/POS networks to authorize transactions if a card issuer or processor is unable to authorize and process transactions, also increase the potential for fraud since normal credit limit and authorization procedures are not in effect. Stand-in authorization arrangements should include reasonable credit limits and defined terms of duration to limit potential financial loss.

Card/PIN Issuance

Financial institutions also assume certain fraud-related risks when issuing credit, debit, and ATM cards either in-house or under contract to third parties. Inadequate internal controls or ineffective card and PIN issuance procedures may result in fraudulent customer transactions. Inappropriate separation of duties that allow employees access to both customer account and PIN information exposes the institution to potential employee fraud.

Embossing and encoding blank plastic card stock, if conducted in-house, should be performed in a secure area and include inventory controls, accounting controls for the number of cards used (including test and reject cards), and dual controls for blank card stock storage. Procedures for the interim storage and accounting of card stock should

exist for all cards not under dual control. Adequate controls should also exist for captured cards (cards confiscated by an ATM machine or elsewhere).

Accountability controls should also be established to ensure all cards initially disbursed from the storage area are either delivered to the mail area or destroyed. Returned cards should be handled by a function independent of the mail department. Control cards should be mailed randomly to customers and their delivery should be validated within a few days to ensure that no theft has taken place.

PIN generation should be done at the time of card issuance. Active PIN information should be controlled, including encrypting the information on storage devices. Access to PIN databases should be restricted on a need-to-know basis. Staff access to PIN information should be reviewed periodically to confirm controls are current and working effectively.

The PIN should not appear in printed form, and staff members should not be able to retrieve or display a customer PIN online. PIN mailers should be processed and delivered with the same level of security used for mailing cards, and an active PIN should never be included with the card mailed to a customer.

The PIN should not be transmitted unencrypted, and the PIN system should record the number of unsuccessful PIN entries, restricting access to a customer's account after a limited number of attempts. If a customer forgets the PIN, he or she should select a new one rather than having staff retrieve the old one.

For institutions that outsource these functions to service providers, written agreements should define roles and responsibilities and detail control and problem resolution procedures. Effective vendor management should include a periodic review of service providers control environments and relevant internal and external audit reports.

Merchant Acquiring

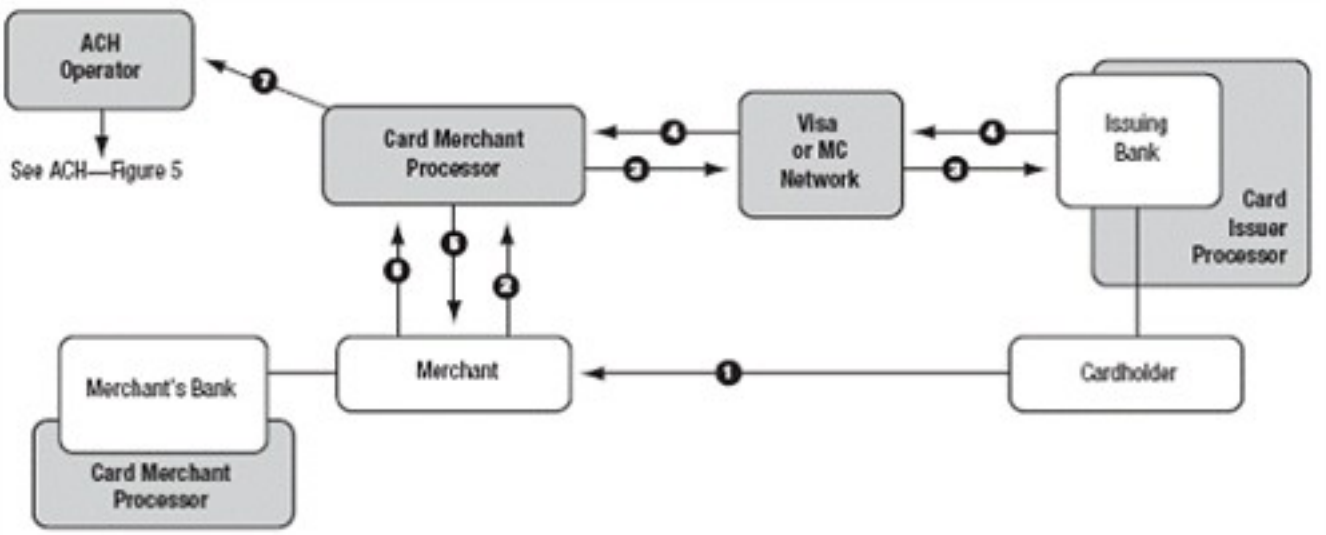
Basic credit card processing participants include the cardholder, cardholder's issuing bank, merchant, merchant's acquiring [51] bank, and the credit card association (e.g., Visa, MasterCard, Discover, AMEX, Diners Club).

Merchants wanting to accept card association-branded credit card sales payments must be sponsored by an acquiring bank that is a member of the credit card association. Merchants may maintain a settlement account with their acquiring bank, or settle via ACH transactions between the acquiring bank and the merchant's bank. Acquiring banks typically do not process their merchants' transactions directly so this function may be outsourced to a third-party service provider (merchant acquirer) that performs the data processing functions of authorization and clearing and settlement. Some merchant banks may also engage the services of an ISO or Member Service Provider (MSP) to solicit and sign up merchants and merchant transaction processing services. Regardless of the presence of such third parties, the credit card networks expect the acquiring bank to be the risk-controlling entity throughout the credit card process. This section will address risks from the acquiring bank's perspective.

The credit card transaction process is initiated when the consumer or merchant swipes the customer's credit card through a POS terminal. The credit approval and payment transaction processing is the same for card-not-present (mail order, telephone order, Internet sales) as they are for card-present transactions. Card-not-present retailers have

additional authentication requirements. The terminal reads and electronically transmits the card number, purchase amount, and merchant ID via the appropriate credit card association network. The credit card association forwards the electronic transaction to the issuing bank or its designated processor to verify that the account is valid and that the customer has adequate credit to cover the purchase. The issuing bank responds back through the network with either an authorization or rejection. Once the merchant receives acknowledgement through the POS terminal, the sale is completed or rejected.

Generally, at the end of each business day, a merchant sends his or her daily charge activity in batch form to his or her acquiring bank or its designated processor who forwards the transaction information to respective credit card associations for clearing. Individual transactions are sent to the issuing banks for customer account processing and debiting of the cardholder's account. Settlement occurs through the card association with the transfer of funds from the issuing banks to the respective merchant's bank. The merchant's acquiring bank posts a credit of the net sales proceeds less interchange and charge-backs to the individual merchant account.



Authorization

1. A consumer uses a credit card to pay a merchant.
2. The merchant sends the encrypted transaction data to a card merchant processor (e.g., First Data Merchant Services) for authorization.
3. The card merchant processor sends the transaction data to the consumer's (issuing) bank over the Visa or MasterCard network. The issuing bank is a licensed member of Visa or MasterCard and holds agreements with, and issues cards to, consumers.
4. The issuing bank authorizes the amount and issues an authorization code or declines the transaction.
5. The card merchant processor notifies the merchant that the transaction either has been authorized or declined. The merchant requests the consumer's signature as authorization for the transaction or notifies the consumer that the transaction has been declined.

Processing

6. Once authorized, the transaction must be "captured" by the merchant. The capture uses information from the successful authorization to charge the authorized amount of money to the consumer's credit card. The merchant accumulates captures and credits into a batch, which then will be settled as a group. The merchant submits the batch to the card merchant processor to finalize the transactions. (If the consumer returns goods after a transaction has been captured, a "credit" is generated.)

Settlement

7. The card merchant processor receives the information and settles the batch, then sends ACH items through the ACH operator to the issuing and merchant banks. (See Figure 5; the merchant bank is the ODFI, with the card merchant processor serving as authorized sending point.) The operator settles transactions between the issuing and merchant banks. The merchant bank credits the merchant's account.

Note: Many merchant banks hire a third party (acquiring processor) for bankcard processing. The processor provides credit card processing, billing, reporting and settlement, and operational services to the merchant bank.

Figure 12: Diagram of typical credit card transaction [52]

As Figure 12 shows, the credit card process is a technology-driven payments process. The payment process relies almost exclusively on the effective application and monitoring of strong technology standards and practices to protect transactional data integrity and to mitigate operational risks across the entire payments network.

Operational and data integrity risks can arise from improper processing of bankcard

transactions, inadequate internal controls, employee error or malfeasance, and other operational challenges inherent when processing within a multi-participant environment. To ensure these risks are mitigated, numerous technological and operational safeguards must be considered when assessing the acquiring banks' abilities to manage and control risks posed by merchants and contracted third-party payment processors.

A key mitigating factor to data integrity risk is the acquiring bank's responsibility to ensure that magnetic-strip data is not retained by merchants and third-party service providers. Many of the publicized data breaches have occurred because merchants and third-party service providers have retained customer sensitive data. Generally it is not acceptable for any participant to retain magnetic-stripe data on a post-transaction basis. Bankcard company rules prohibit-post transaction storage of full-track data (Track 1 and Track 2), CVV2/CVC2/CID/CAV, and, if applicable, the PIN block. CVV2/CVC2/CID/CAV are terms used by the various bankcard companies to refer to a unique check value that is printed on the back of the card and/or encoded in the magnetic strip. Track 1 and Track 2 data is encoded on the magnetic strip and contain information such as account number, cardholder's name, card expiration date, and service codes. Merchants and third-party service providers are allowed to store the cardholder's name, account number, and expiration date on a post-transaction basis as long as the information is encrypted, hashed, or truncated. Merchants and third-party service providers should have transaction data access protected using strong passwords and should have all data-access activity logged and available for independent review. Servers holding cardholder data should be hardened to minimize the risk of unauthorized access. Cardholder data should never be stored on a server connected to the Internet.

Historically, merchant responsibility for reporting a data breach has not been governed universally by any one entity, law, or set of guidelines other than bankcard company rules. In recent years, many states have passed legislation with various requirements for merchants reporting data breaches and various forms of financial liability.

Merchants relying on Web-based applications to conduct business should ensure that the applications are developed using IT industry secured-coding guidelines. All sensitive data transmitted via public networks must be encrypted using IT industry-standard encryption or higher. This also applies to all wireless transmissions, especially at the merchant retail level. Retail card payments containing sensitive customer information and processed using an unencrypted wireless transmission have been captured by fraudsters simply by sitting in the retailer's parking lot with a laptop computer.

Acquiring banks are ultimately responsible for any risks posed to the payment system by their sponsored merchants and third-party service providers. Management and the board of directors of all participants, including the acquiring banks, must have a clear understanding of the risk associated with acquiring activities and must understand their obligations under credit card association rules.

The credit card associations require acquiring banks to ensure that their merchants and third-party service providers comply with the Payment Card Industry Data Security Standards (PCI DSS). For third-party service providers and large merchants, PCI DSS compliance validation must be performed annually by a Qualified Security Assessor that has been approved by the PCI Security Standards Council. Smaller merchants must validate compliance annually through completion of a self-assessment questionnaire. It is not uncommon within the industry for a large number of merchants, and even some third-party service providers, to be in noncompliance with PCI DSS, potentially exposing their acquiring bank to reputation risk and financial loss from fraud, lawsuits, and fines. Additionally, issuing banks that use third-party service providers for transaction

processing are required by the card associations to ensure that their providers are in compliance with PCI DSS.

There are six categories of PCI compliance security standards. [53]

Build and Maintain a Secure Network

Requirement 1: Install and maintain a firewall configuration to protect cardholder data.

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters.

Protect Cardholder Data

Requirement 3: Protect stored cardholder data.

Requirement 4: Encrypt transmission of cardholder data across open, public networks.

Maintain a Vulnerability Management Program

Requirement 5: Use and update regularly anti-virus software.

Requirement 6: Develop and maintain secure systems and applications.

Implement Strong Access Control Measures

Requirement 7: Restrict access to cardholder data by business need-to-know.

Requirement 8: Assign a unique ID to each person with computer access.

Requirement 9: Restrict physical access to cardholder data.

Regularly Monitor and Test Networks

Requirement 10: Track and monitor all access to network resources and cardholder data.

Requirement 11: Test security systems and processes regularly.

Maintain an Information Security Policy

Requirement 12: Maintain a policy that addresses information security.

In addition to protecting cardholder information, the credit card payment process requires acquiring banks to maintain strong credit practices over their commercial customers (merchants). The credit risk incurred by acquiring banks is similar to that of ACH ODFIs in that the acquiring bank bears the financial obligation if the merchant fails to pay.

As with any line of credit, acquiring banks are responsible for ensuring credit screening of current and prospective merchants. The acquisition of new merchants is called "merchant boarding" and may be done by the acquiring bank or, more frequently, by a third party such as an ISO. The acquiring bank is responsible for due diligence of new merchants regardless of whether the bank or a third party performs the merchant boarding. The screening process should include physical inspection of premises; a credit history review; background check; and a review of business plans and operations, including projected sales volumes, chargeback activity, and type of sales (card-present or card-not-present). For online merchants, the screening process should include a

review of Web site content and functionality. Additionally, phone, mail and Web-based merchants should be monitored closely to ensure no illegal or high-risk business activity is being conducted. Of particular concern are Web sites that present higher levels of repudiation rates which could result in higher levels of credit losses.

The main source of credit risk to acquiring banks are chargebacks resulting from cardholder disputes that merchants cannot honor. When the merchant is unable to pay its chargebacks due to bankruptcy or fraud, the acquiring bank must cover the chargeback and pay the issuing bank. Acquiring banks should manage carefully the merchant portfolio and employ appropriate underwriting, chargeback processing, and fraud monitoring.

The acquiring bank is also ultimately responsible for credit and fraud risks presented by merchant accounts acquired through ISOs or MSPs. The ISO or MSP cannot be a member of a credit card association but can represent an acquiring bank in a merchant relationship. Acquiring banks must register their ISOs or MSPs with the credit card associations, and a written merchant agreement must be in place outlining the relationship, roles, responsibilities, and liability of each of the parties - ISO or MSP, merchant, and merchant acquirer.

Acquiring banks have a number of options to monitor and control credit risks in order to minimize fraud losses at the merchant level. Acquiring banks should have reports providing information such as: average sale-ticket size for the business being conducted, chargeback level and frequency, inactive merchants, percentage of manually keyed transactions to total transactions, same dollar amounts in submitted batch, large number of even dollar-amount transactions, increasing percentage of declined or referred authorizations to total sales, and continuous or frequent zero balance in DDA accounts. These reports may also be useful for identifying potential money laundering red flags.

If an acquiring bank has concerns regarding a merchant, it has the ability to delay funding, install a front-end fraud monitoring system, acquire bank statements and credit reports, and visit the merchant's place of business. Acquiring banks can also require a reserve balance be held, generally as a percentage of credit card receipts, and it can require the merchant to purchase chargeback insurance.

Examiners should assess the actions the acquiring bank has taken to ensure third-party service providers, ISOs or MSPs, and merchants are protecting the bank's interest.

EFT/POS and Credit Card Networks

Financial institutions should have accurate audit trails for all transactions at each network switch point. The audit trails should identify the originating terminal and destination. To ensure accurate transaction posting, the financial institutions should have adequate procedures in place to control transaction activity if the EFT/POS network becomes inoperable. Also, financial institutions should document and monitor procedures for balancing and settling transactions to ensure that they adhere to interchange policies. Each participant in the switch should receive adequate transaction journals and exception reports necessary to facilitate final settlement for the institution.

A financial institution should establish stand-in processing arrangements with peer financial institutions as part of its disaster recovery and business continuity plans to ensure availability of the service. Additionally, it should have adequate oversight and

contract provisions for all outsourced services to ensure continuity of expected service levels. Agreements between switch or network participants should delineate each party's liabilities and responsibilities. The agreements should detail basic control items concerning normal and contingency processing and assign responsibility for corrective action. Grievance procedures and arbitration policies are also an important part of participant agreements.

Internet and Telephone-Initiated ACH

Financial institutions originating ACH debit entries through the Internet should ensure they are in compliance with NACHA requirements. NACHA rules establish a WEB standard entry class (SEC) code for Internet-initiated ACH debit entries to which a number of requirements apply. The rules apply to originators and also affect the ODFI and its service providers. Under these rules, financial institutions must use the WEB SEC code to identify all ACH debit entries to consumer accounts that a receiver authorizes through the Internet. This code applies to both recurring and single entry ACH debits. In addition, an ODFI that transmits WEB entries must warrant that its originators have met certain NACHA standards.

Financial institutions offering TEL origination services on behalf of their customers are exposed to substantial risk from merchants that may be engaged in fraudulent or deceptive business practices. Therefore, these institutions should adopt applicable NACHA risk management practices.

Endnotes

[1]	This booklet uses the terms "institution" and "financial institution" to describe an insured bank, savings association, and credit union, as well as TSPs providing services to a financial institution.
[2]	This booklet references specific services and brand names including those trademarked by their respective companies. These references are intended solely to provide a retail payment systems overview and should not be construed as an FFIEC endorsement of any product or service noted herein.
[3]	www.ffiec.gov/exam/check21/.
[4]	See "Nonbanks in the Payments System," March 6, 2003, and "A Guide to the ATM and Debit Card Industry," April 7, 2003, describing payment flows and clearing and settlement arrangements at: www.kansascityfed.org/home/subwebnav.cfm?level=3&theID=10724&SubWeb=10658#2003.
[5]	NACHA is the body that establishes the rules and procedures governing the exchange of automated clearinghouse payments.
[6]	This booklet addresses the risks and controls associated with the bill payment transaction. See the IT Handbook E-Banking Booklet for the risks and controls associated with the front-end bill payment application used to initiate bill payments.
[7]	Interoperability refers to the ability of diverse retail payment systems to exchange data with a minimal loss of integrity. Many retail payment systems lack consistent protocols defining the data and the data fields in each system. Consequently, data cannot be readily moved from one system to another without manipulation.
[8]	For further information, see the American National Standards Web site at www.ansi.org/.
[9]	Truncation is the process of removing a paper check from its processing flow. In truncation, both sides of the paper check are scanned to produce digital images. If a paper document is needed, these images are inserted into specifically formatted documents containing a photo-reduced copy of the original checks called a "substitute check."
[10]	The term "bank" includes any depository institution as defined in 12 U.S.C. 461 (b)(1)(A).
[11]	See www.ffiec.gov/pdf/pr011409_rdc_guidance.pdf for FFIEC Guidance on Risk Management of Remote Deposit Capture.
[12]	It is important to note that check conversion requires appropriate disclosures to the check writer and is not available for all checks.

[13]	A remotely created check (sometimes called a "demand draft") is a check, often created by a payee or its service provider, drawn on a customer's bank account. The check often is authorized by the customer remotely, by telephone or on-line and therefore does not bear the customer's handwritten signature.
[14]	A demand draft created by the paying bank is not an RCC. See definition of RCC in Regulation CC.
[15]	The "midnight deadline" for the return of a check is midnight on the next banking day following the banking day on which the check is presented.
[16]	See www.frbservices.org/files/regulations/pdf/operating_circular_3.pdf for Operating Circular No. 3: Collection of Cash Items and Returned Checks, effective July 15, 2008.
[17]	See www.ffiec.gov/pdf/pr011409_rdc_guidance.pdf for FFIEC Guidance on Risk Management of Remote Deposit Capture.
[18]	See www.ffiec.gov/bsa_aml_infobase/default.htm.
[19]	See the IT Handbook Wholesale Payment Systems Booklet for a discussion of Fedwire®.
[20]	See www.frbservices.org/nationalsettlement/index.html.
[21]	Check authorization is typically performed by a third-party service provider.
[22]	The original or a qualifying substitute check is needed for presentment unless agreed to otherwise.
[23]	See www.nacha.org/ for further information on NACHA.
[24]	EPN is a subsidiary of The Clearing House (formerly known as the New York Clearing House Association).
[25]	See www.frbservices.org/files/regulations/pdf/operating_circular_4.pdf for Federal Reserve System Operating Circular No. 4 on "Automated Clearing House Items."
[26]	NACHA typically uses the acronym TPSP to designate third-party service providers. Generally, TPSPs are not the same as technology service providers (TSPs), the term the FFIEC uses to denote third-party entities that provide technology services to financial institutions. It is possible that a particular TPSP may also be a TSP, but for the purposes of this booklet, no such connection is made.
[27]	See NACHA International Transactions Executive Summary: http://www.nacha.org/IAT_Industry_Information/docs/IAT%20Executive%20Summary%207%203108.pdf

[28]	The ODFI reporting requirements also requires ODFI to provide NACHA with information pertaining to each originator or 3rd party sender return rates which exceed a defined threshold.
[29]	More information about these rule changes and other developments, including proposed rules changes and pilot projects, may be found at the NACHA Web site: www.nacha.org.
[30]	"Merchant acquirer" is a broad term used to describe a number of industry participants including third-party service providers, independent sales organizations (ISOs), and other agents. The operating regulations of the major payment card networks require these nonbank entities to be sponsored by a member financial institution (acquiring bank) and to register with the payment network.
[31]	For purposes of this booklet, the bankcard systems, MasterCard and Visa,, are referenced interchangeably as companies and associations.
[32]	Some private label (store) credit card retailers actively manage card issuance and credit relationships through affiliated financial institutions.
[33]	Non-financial institution processors must be sponsored by financial institutions to process merchant transactions.
[34]	Each business day, the association's settlement financial institution receives information from the association about issuer and acquirer positions, sending Fedwire® 1031 draw-down messages to all of its issuers with instructions to fund their settlement accounts for those amounts. The association's settlement financial institution debits issuer accounts for those amounts and credits the appropriate acquiring financial institution accounts. If an issuer does not fund its account on time, the association will intercede, cover the short position, and assess a penalty fee on the issuer.
[35]	NACHA Rules Interpretation: Proper Use of SEC Codes and Aggregation of Transactions, Issued November 9, 2007, effective: August 4, 2008. This interpretation provides that transactions may not be aggregated unless specific circumstances exist; specifically, they must be aggregated under the WEB or PPD codes if the transactions are accumulated in an account for more than 14 days.
[36]	FFIEC Guidance "Authentication in an Internet Banking Environment," October 2005 www.ffiec.gov/press/pr101205.htm
[37]	See http://irda.affiniscape.com/associations/2494/files/Publications/FM_Exec_Summary.pdf
[38]	See the IT Handbook Outsourcing Technology Services Booklet.
[39]	For more details, see www.federalreserve.gov/paymentsystems/psr/relpol.htm.

[40]	See the IT Handbook Wholesale Payment Systems Booklet for additional information on National Settlement Service and PSR policy.
[41]	See the IT Handbook Management Booklet
[42]	Insured depository institutions are subject to Regulation F (Limitations on Interbank Liabilities, 12 CFR Part 206) which requires institutions to monitor and limit their exposures to correspondents.
[43]	See the IT Handbook Audit Booklet.
[44]	More information on PCI Data Security Standards may be found at the website: www.pcisecuritystandards.org.
[45]	FFIEC Guidance "Authentication in an Internet Banking Environment," October 2005 & "Authentication in an Internet Banking Environment - Supplement" June 2011.
[46]	See the IT Handbook Business Continuity Planning Booklet.
[47]	See the IT Handbook Outsourcing Technology Services Booklet.
[48]	See the IT Handbook Outsourcing Technology Services Booklet.
[49]	The ACH operator usually requires an authorization from the ODFI before processing a file. Failure to receive ODFI authorization will result in the ACH operator deleting the file, giving the ODFI control over its exposure from files originated or subsequently changed by a TSP.
[50]	Automated Clearing House Rules: Article 2.1.1, Article 5.2, and Article 5.3.
[51]	Some industry publications include service providers, ISOs, and other agents in their definition of a merchant acquirer. Regardless of the term used, all participants require sponsorship by a member financial institution also known as the acquiring bank.
[52]	Source: Nonbanks in the Payments System, 2003, page 24, Federal Reserve Bank of Kansas City.
[53]	PCI Security Standards Web site: www.pcisecuritystandards.org.
[54]	A mobile device is a portable computing and communications device with information-storage capability.
[55]	The mobile channel refers to providing banking and other financial services through mobile devices.

[56]	A mobile wallet is a front-end application that stores payment card information on the mobile device and allows payments to be made using a mobile device. The mobile wallet utilizes traditional retail payment channels such as ACH, EFT, and debit/credit card networks to process the payments.
[57]	A QR code is a type of two-dimensional bar code or machine-readable optical label that contains information about the item to which it is attached.
[58]	Closed-loop payments allow consumers to pre-load funds into a spending account that is linked to the payment device that can be used for purchases only at a specific company. Open-loop payments allow consumers to tie a mobile wallet to a personal account (e.g., credit card), do not require a prepaid amount, and spending is not limited to one company.
[59]	Funding refers to adding a positive balance that customers use to make purchases.
[60]	Traditional payment risks associated with the underlying payment transaction are covered by existing risk management guidance contained in earlier sections of this booklet.
[61]	Access points include a user's home network, cellular network, NFC, Bluetooth, or public Wi-Fi connections, such as those provided by a municipality or business.
[62]	SMS spoofing is the manipulation of address information to impersonate a user.
[63]	Vulnerabilities include malware attacks, eavesdropping, and spoofing.
[64]	Besides e-mail and instant messages, sources can also include SMS, social messengers, hypertext markup language (HTML) links, and QR codes.
[65]	Anti-phishing software are programs, either integrated with or built in to the Web browser, that display the real domain name of the site that a user is visiting to help prevent fraudulent sites from posing as legitimate sites.
[66]	Anti-XSS functionality is a defense mechanism to XSS, which is a vulnerability found in Web applications that enables attackers to inject client-side script into Web pages prompting a Web page to display unvalidated user input. Attackers may use this vulnerability to bypass access controls.
[67]	Unvalidated Web site redirects are possible when a Web application accepts untrusted input that could cause the application to redirect the request to a malicious URL. A user may be redirected and not realize it.
[68]	URL is an acronym for uniform resource locator and is a reference (an address) to a resource on the Internet.

[69]	The root user is the conventional name of the user who has all rights or permissions to all files and programs. Having such rights or permissions allow the root user to do many things an ordinary user cannot.
[70]	Refer to U.S. Secret Service and PCI Security Standards Council, "Joint Advisory Bulletin: Mobile Payment System Vulnerability," September 2015.
[71]	Personalization is providing a tailored user experience based on user preferences through MFS.
[72]	Out-of-band refers to activity outside of the primary means of interfacing with the customer. For example, if a user is performing activity online, he or she may be authenticated through a one-time password sent via text message.
[73]	Resources that provide detailed information about authentication for financial institutions include: FFIEC Authentication Guidance (http://www.ffiec.gov/pdf/authentication_guidance.pdf), Frequently Asked Questions (https://www.ffiec.gov/pdf/authentication_faq.pdf), and Authentication Supplement (https://www.ffiec.gov/pdf/Auth-ITS-Final%206-22-11%20(FFIEC%20Formated).pdf).
[74]	Threat modeling is a structured approach that enables an institution to aggregate and quantify potential threats. In the context of application development, threat modeling can be used to capture, organize, and analyze all of the threat information of an application and its environment that affects application security. It is used to enable informed decision-making about application security and helps to produce and rank a list of security improvements.
[75]	Secure coding is the process of developing code (e.g., Web application) with security built in during the development process using technical controls to mitigate the occurrence of software vulnerabilities.
[76]	White-hat hacking, also called ethical hacking, refers to the specialization of penetration testing and other testing methodologies to review the security of an institution's information systems by determining flaws and vulnerabilities.
[77]	Prudent security practices may include information on the use of the device's password function, general safeguards, and any additional logical security controls (e.g., available security applications).
[78]	OWASP is an online community dedicated to Web application security.
[79]	A whitelist is a list of trusted entities. With respect to URL redirects, an institution can create a whitelist of allowable URLs.
[80]	A sandbox is a restricted, controlled execution environment that prevents potentially malicious software, such as mobile code, from accessing any system resources except those for which the software is authorized.

[81]	The goal of a denial-of-service attack is to restrict the availability of services or systems. If the institution can effectively filter traffic to disallow unknown or potentially malicious traffic, this can support the institution's larger denial-of-service planning.
[82]	The trusted platform module is an international standard for a secure crypto processor that is a dedicated microprocessor designed to secure hardware by integrating cryptographic keys into devices.
[83]	Tokenization is the process of substituting a sensitive data element with a surrogate value, referred to as a token.
[84]	Statement on Standards for Attestation Engagements (SSAE) No. 16 is a type of audit report of controls at a service organization.
[85]	A review should include the financial institution's consideration of expectations set forth in appropriate supervisory guidance (e.g., authentication guidance in footnote 20 of this appendix).
[86]	Uniform Rating System for Information Technology.

Appendix A: Examination Procedures

EXAMINATION OBJECTIVE: Examiners should use the following Tier I and Tier II Retail Payment Systems examination procedures to evaluate the policies and procedures, business processes, personnel, and internal control systems of financial institutions and technology service providers. Retail payment system services include checks and share draft item processing, bankcards, payment cards, ACH, EFT/POS networks, electronic bill payment, person-to-person (P2P) and account-to-account (A2A) payment systems, and many other products and services resulting from emerging advances in technology. The examination scope should be based upon the risk profile of the financial institution or the technology service provider. The risk profile is determined through an assessment of the entity's risk environment and quality of risk management practices. This assessment should consider the formal policies and procedures established to provide these services, as well as the effectiveness of the financial institution's underlying internal control environment, including information security, business continuity, disaster recovery, and vendor management programs.

Retail payment services expose financial institutions to numerous risks, including legal, compliance, strategic, operational, credit and liquidity. Depending on the complexity of retail payment system activity, the scope of the examination may require an integrated team approach that includes the knowledge, skills, and expertise of, IT, credit, and compliance specialists.

The examination procedures may be part of either an IT or safety and soundness examination. Examiners can use the procedures in their entirety or in a modular fashion to focus on particular retail payment system products, services, or business lines. Depending on the size, complexity and risk profile of the financial institution or technology service provider, not all of the procedures may be necessary to develop overall conclusions. The examination of retail payment services may also support the institution's BSA/AML examination, which requires an evaluation of related risks in retail payment services.

The primary objectives of the Tier I procedures are to evaluate the effectiveness of the internal controls and risk management processes implemented by the financial institution or the technology service provider. Examiners should use the Tier II procedures to expand the scope of the examination further if the risk profile or organization's complexity requires additional information to establish comprehensive and accurate examination conclusions.

TIER I OBJECTIVES AND PROCEDURES

Objective 1: Assess the level of risk in retail payment systems function.

1. Determine the types of retail payment products and services offered. Consider the following:

- The types of customers using the products and services.
- The geographic service footprint (e.g., international usage)
- Check processing, particularly check imaging, remotely created checks (RCCs), and remote deposit capture
- ACH, including third-party originations, TEL, WEB, ARC, POP, and BOC
- Card issuance
- Card processing
- Merchant acquisition and processing

2. Determine whether new retail payment products and emerging technologies pose increased risk due to the lack of maturity of the respective control environments. Consider:

- New retail payment products and services that have been introduced within the past year.
- Whether the institution introduced any existing products into new markets within the past year.

3. Determine if the quality of management and staff, and the staffing levels are adequate for the specific retail payment products and processes the institution provides.

- Obtain and review the following:
  - Reports showing staffing levels, turnovers, and trends.
  - Biographies of managers and key staff
- Consider:
  - The levels of skill and experience of key managers and staff, particularly in terms of the sophistication and complexity of the products, processes, and systems.
  - Whether the institution has appropriate depth of management and staff.
  - The adequacy of staffing levels for peak operating periods.

    Management and staff turnover.

4. Determine if the quality of process design and control points are adequate for existing retail products, and if these factors are considered for new products. Consider whether:

- There is adequate capacity for current and planned transaction volumes.
- Processes are clearly designed.
- Processes are automated.
- There is a reasonable degree of manual intervention.
- Any processes have been re-engineered during the past year.
- Processes are outsourced or performed at the customer location.

5. Evaluate the use of in-house and outsourced data processing systems to support retail payment products and processes. Consider:

- How stable are existing systems.
- How current are existing systems.
- Whether there is adequate capacity for current and planned transaction volumes.
- Whether the institution uses leading edge technologies or only mature technologies.
- To what extent are systems outsourced.
- Whether outsourcing arrangements are governed by contracts and service level agreements.
- Whether vendors are considered to be industry-recognized leaders.

Objective 2: Establish the scope and objectives of the examination of the retail payment systems function.

1. Review previous reports of examination for comments relating to retail payment systems. Review:

- Regulatory reports of examination, including consumer and compliance information.
- Prior examination work papers, including any documentation obtained through on-going supervision.
- Internal control self-assessments completed by business lines.
- Internal and external audit reports, including annual attestation letters.
- Regulatory, audit, and information security reports from service providers.

- Trade group, bankcard company, interchange, and clearing house documentation relating to services provided by the financial institution, particularly the NACHA required annual security audit and bankcard company self assessments.
- Supervisory strategy documents, including risk assessments.

2. Review past examination reports for comments relating to the institution's internal control environment and technical infrastructure. Review:

- The institution's processing architecture, including processing outsourcing arrangements.
- Internal controls, including physical and logical access controls in the data entry area, data center, and item processing operations.
- Electronic Funds Transfer (EFT)/Point of Sale (POS) network controls.
- Comments related to controls over Remote Deposit Capture (RDC).
- Inventory of computer hardware, software, and telecommunications protocols used to support check item processing, EFT/POS transaction processing, ACH, and bankcard issuance and acquiring transaction services.

3. Review the financial institution's risk and control assessments for comments relating to retail payment systems. Review the following risk assessments:

- External and internal audit;
- Management controls;
- Information security;
- Business continuity;
- Regulatory compliance; and
- BSA/AML.

4. Identify and obtain during discussions with management of financial institution or service provider:

- A description of the retail payment system activities performed and scope of operations, including check item processing, RDC, lock-box services that provide ACH check conversion or check truncation, ACH, bankcard issuing and acquiring,

clearance, settlement, and EFT/POS network activity.

- Operational reports for retail payment system activities, including transaction volumes, dollar amounts, and trends. Where possible, compare levels and trends with peer financial institutions. Significant increases may indicate a change in risk to the financial institution and management awareness should be evaluated.
- Organization charts of retail lines of business to determine reporting relationships and how the collective retail lines of business are structured and managed.
- The retail payment system functions performed through outsourcing relationships and the financial institution's level of reliance on those services.
- Any significant changes in retail payment system policies, personnel, products, strategy and services since the last examination, particularly the introduction of new and emerging electronic retail payment systems incorporating RDC, wireless, telephone, web-based purchasing and bill payment, prepaid cards, or P2P and A2A payment systems.
- A listing of all payment processing and clearing house settlement arrangements in which the financial institution participates. Include any bilateral retail payment clearing arrangements the institution may have with other institutions that are outside traditional clearing houses such as FedACH and EPN. Evaluate the methodology used by the financial institution in assessing its operational and settlement risk from these arrangements.
- Documentation of any related operational or credit losses incurred, reasons for the losses, and actions taken by management to prevent future losses for each retail payment system.
- A network diagram of the transaction flow from the merchant end of the network, through any intermediary processors, to the financial institution, for all types of payment channels.

5. Review the financial institution's response to any retail payment systems issues raised at the last examination and any internal audits conducted since last review. Determine:

- Adequacy and timing of corrective action.
- Resolution of root causes rather than specific issues.
- Existence of outstanding issues.

Objective 3: Assess the quality of oversight and support provided by the board of directors and management.

1. Determine the quality and effectiveness of the financial institution's retail payment systems management function. Consider:

- The alignment of the institution's business plans with its technology and operational plans for retail payment systems.
- Data center and network management and the quality of internal controls over internal ATM networks and gateway connectivity to regional, national, and international EFT/POS and bankcard networks.
- Departmental management and the quality of internal controls, including separation of duties and dual control procedures, for bankcard, ATM and debit card, ACH, check items, and electronic banking payment transaction processing, clearance, and settlement activity.
- Departmental management and the quality of information security and GLBA 501(b) compliance policies relating to retail payment system-generated customer data.

2. Assess management's ability to manage outsourced relationships with technology service providers. Consider:

- Process utilized to encrypt transactions while in route between technology service providers and the institution.
- Adequacy of contract provisions including service level, performance agreements, responsibilities, liabilities, and management monitoring.
- Management's determination of the service provider's compliance with applicable financial institution and consumer regulations and with third-party requirements (e.g., NACHA, GLBA, bankcard company, and interchange).
- Adequacy of contract provisions for personnel, equipment, and related services.
- Quality of management information systems (MIS) and reports needed to monitor the technology service provider's performance appropriately.

3. Evaluate the adequacy and effectiveness of financial institution and service provider contingency and business continuity planning. Consider:

- Ability to recover transaction data and supporting books and records based on retail payment system business line requirements and time lines.
- Level of testing conducted to ensure adequate preparation.
- Stand-in arrangements established with other financial institutions in the event of an ATM and/or POS system outage. preventing card fraud and abuse.
- Alternative access mechanisms in the event of an outage to primary access to bankcard, ACH, and other retail payment networks.

4. Evaluate retail payment system business line staff. Consider:

- Adequacy and quality of staff resources, including certifications such as an Accredited ACH Professional (AAP).
- Effectiveness of policies and procedures outlining department duties, including job descriptions.

Objective 4: Assess the quality of policies, procedures, and limits supporting retail payment services.

1. Review policies, procedures, and limits for supporting all retail payment services.

- Determine if there are written policies.
- Determine if the policies reflect the current business and processes.
- Determine if the policies establish reasonable limits.

2. Review staff training programs and determine if they are appropriate for supporting policies.

3. Determine whether the institution monitors compliance with policies, procedures, and limits.

- Determine if exception monitoring reports are elevated to appropriate levels of management.

Objective 5: Assess the quality of management information systems and reports used to manage retail payment services.

1. Review management reports for all retail payment services including reports from service providers.

- Determine if the reports are appropriate to the businesses and processes in terms of scope and frequency.
- Determine if the reports are reviewed at the appropriate levels of management.

Objective 6: Assess the quality of risk management and support for bankcard issuance and acquiring (merchant processing) activity.

1. Evaluate financial institution adherence to bankcard company rules and bylaws and regulatory requirements.

2. Evaluate whether card issuance processing is outsourced to a third party. If yes, evaluate the vendor management controls in place to govern the activities listed in steps 3 and 4.

3. Review internal procedures employed for each bankcard product and assess:

- The integrity of plastic card and PIN issuance processing.
- Whether processing includes appropriate separation of functions in card issuance, PIN issuance, control and storage of card stock, and the maintenance of software controlling PIN generation.
- Whether the institution has established procedures focusing on controls preventing card fraud and abuse.

4. Determine whether the audit function periodically performs an inventory of all bankcards at each location owned or operated by the institution and that each location is included in the audit program, either directly or indirectly (e.g., as part of a branch audit).

5. Determine whether management has established inventory systems that include quality control activities such as self-monitoring for data accuracy.

6. Review a sample of consumer contracts for each bankcard service to ensure they describe adequately the responsibilities and liabilities of the institution and its customers (compliance with Regulation Z).

7. Evaluate the effectiveness of internal clearance and settlement activity as it relates to customer bankcard transactions. Consider the adequacy of:

- Financial and accounting controls in place to clear and settle transactions.
- Periodic reconciliation of all account postings.
- Timely clearance or charge-off of missing items or out-of-balance situations.

8. Evaluate the effectiveness of internal credit monitoring and card authorization performed by the financial institution. Consider the adequacy of:

- Policies and procedures for underwriting, account management, and collection activities.
- Card authorization procedures to mitigate fraudulent use.

- MIS reports and behavioral fraud analysis.

9. For financial institutions directly involved in, or outsource, bankcard acquiring (merchant processing) services, determine the appropriateness of controls over merchant services and ISO/MSP relationships. Consider the adequacy of:

- New merchant approval and acceptance process, termination procedures, and underwriting guidelines for merchant accounts with particular attention to Web and telephone-based businesses.
- Testing of web-based business to validate site's content.
- Industry-standard MIS reports to identify negative trends and potential fraudulent activity. Potential indicators of fraud or money laundering include: a large number of manually keyed transactions, even dollar amount transactions, average sale ticket size as compared to history, same dollar amount repeated frequently in a single batch, or continuous or frequent zero balances in DDA account.
- The financial institution's use of a front-end fraud detection application either in-house design or purchased.
- Credit approval and monitoring procedures for all new and established merchant accounts. Consider use of Dun & Bradstreet reports, bank statements and credit reports.
- Chargeback processing procedures and controls, including trend, volume, age, and losses associated with merchant chargebacks.
- Agent bank programs (where the financial institution performs merchant processing for other institutions), and the level of liability assumed by the acquiring financial institution.
- Protection and storage of cardholder data and compliance with card company rules and guidelines on what data can and cannot be stored.
- Programs for requiring and monitoring merchant's and processor's compliance with card company and association standards such as PCI Data Security Standards. Review assessment document and process for completion.
- Policies and procedures relating to customer accounts that may have been the subject of security breach at the merchant/ISO location (i.e., reissue cards, monitoring and customer notification).

Objective 7: Assess the quality of risk management and support for EFT/POS processing activity.

1. Evaluate the financial institution's compliance with interchange rules and bylaws.

2. Review internal procedures employed for generating active ATM cards. Consider:

- The integrity of PIN issuance and processing, including appropriate separation of functions between card issuance, PIN issuance, and card stock control and storage.
- The maintenance of software controlling PIN generation. The review should focus on controls preventing card fraud and abuse resulting in financial loss to the institution.

3. Determine whether the audit function periodically performs an inventory of unused ATM card stock at each location owned or operated by the institution and that each location is included in the audit program, either directly or indirectly (e.g., as part of a branch audit).

4. Review a sample of consumer contracts for ATM services to ensure they adequately set forth responsibilities and liabilities of the institution and the customer. Evaluate compliance with applicable regulations.

5. Evaluate the effectiveness of internal clearance and settlement activities as it relates to customer ATM transactions. Consider whether:

- Appropriate financial and accounting controls are in place to clear and settle ATM transactions.
- Reconciliation is performed periodically for all account postings.
- Processes have been established for handling disputed items.

Objective 8: Assess the quality of risk management and support for ACH processing activity.

1. Evaluate the financial institution's adherence to NACHA and clearing house operating rules and regulations.

2. Review operational reports showing monthly or quarterly ACH debit and credit activity and, if possible, compare levels with peer financial institutions. If ACH activity is greater than peer, determine whether institution is an originating institution (ODFI). Obtain reports listing those customers for which they originate and the volumes (number of items and dollars) originated. Be sure to ask for all customers that use the ODFI's originating account number with the Federal Reserve or EPN.

3. If the institution has bilateral clearing arrangements with other institutions, review the underlying contracts and determine how the institution monitors compliance with the contracts.

4. If the institution uses a technology service provider, determine whether it performed appropriate due diligence prior to engagement and has appropriate contractual agreements governing the relationship. Determine whether the institution monitors compliance with the governing contract. Determine if the institution has an adequate business continuity plan in the event the technology service provider experiences a service disruption.

5. If the institution is an ODFI and permits third-party sender payments, determine whether it requires the third-party sender to establish the identity of each originator using commercially reasonable methods to warrant that the originators will assume their responsibilities under NACHA rules and to warrant that it will assume the liabilities of the ODFI. Determine whether the ODFI has established limits and monitoring of the third-party sender's creditworthiness relative to its underlying originators and the nature and type of ACH activity that it warrants.

6. Determine whether the ODFI's contractual agreements with each originator clearly define the specific terms for funds availability.

7. Determine whether the institution has taken steps to ensure that originators are properly educated about their obligations for handling ARC and POP source documentation and all other NACHA rules.

8. Review policies and procedures for acquisition of originating customers and determine the appropriateness of these policies for the risk profile and risk management capabilities of the financial institution. Determine whether the policies identify and seek to limit exposure to higher risk customers; such as, adult entertainment and online gambling firms, adult bookstores, escort services, and massage parlors.

9. Review policies and procedures in place to monitor originating customer balances for credit payments (e.g., payroll) to ensure payments are made against collected funds or established credit limits and daily caps. Also determine whether payments in excess of established credit limits and daily caps are properly authorized.

10. Determine whether the institution treats deposits resulting from ACH transmitted debits on other accounts as uncollected funds until there is reasonable assurance the debits have been paid by the institution on which they were drawn. Also, determine whether management monitors drawings against uncollected funds to ensure they are within established guidelines.

11. Review a sample of contracts authorizing the institution to originate ACH items for customers and determine whether they adequately set forth the responsibilities of the institution and customer. Determine:

- Whether contracted technology service providers originating customer entries are also customers of the financial institution.
- Whether the agreements include recognition of all relevant NACHA requirements.
- Whether ACH clearing houses, of which the financial institution is a member, stipulate the funding arrangements (outgoing), Expedited Funds Availability Act (Regulation CC), UCC Article 4A (credit transfer only), and Electronic Funds Transfers (Regulation E).

12. Determine whether the institution has a process in place for monitoring and acting on returned items, that includes third-party vendors, where applicable..

13. Determine whether the institution uses risk management reports that are appropriate to the ACH activities and level of risk.

14. Determine whether ACH activities are considered in the institution's overall business continuity plans and insurance program.

15. Determine whether management monitors originating customers for unreasonable numbers of unauthorized ACH debits. If the volume of unauthorized ACH debits is high, it could expose the institution to greater loss.

16. Determine whether management has addressed international ACH requirements, where applicable.

Objective 9: Assess the quality of risk management and support for electronic banking related retail payment transaction processing.

1. Determine the extent to which the financial institution engages in retail payment systems, including bill payment, prepaid cards, wireless systems, contactless payment devices, remote check capture, lock-box services that provide ACH check conversion or check truncation, and P2P and A2A payments. Consider:

- Strategic plans relating to the introduction of new retail payment system products and services.
- The development of internal pilot programs and partnerships with technology service providers introducing new retail payment systems and delivery channels.
- The extent to which existing Internet and e-banking products and services include new retail payment mechanisms.

2. Evaluate the financial institution's ability to manage the development and implementation of new retail payment services, focusing on effectiveness of internal controls and provisions of consumer compliance regulations. Consider:

- Information security, including identification and authentication systems, in the deployment of any smart cards, wireless payment devices, EBPP, P2P and A2A product offerings.
- Customer disclosure and compliance information for retail payment systems using new technologies.
- Technical resources to effectively manage retail payment systems including Internet technologies, telecommunications protocols, and operations support.

3. Evaluate the financial institution's ability to incorporate new retail payment product offerings into its existing retail business lines and its effectiveness in including these product offerings in its traditional retail payment operations. Consider:

- The integration of new retail payment product offerings into existing clearance,

settlement, and accounting functions.

- Whether the financial institution relies on technology service providers for some or all of these services.

Objective 10: Assess the quality of risk management and support for checks.

1. Determine whether the accounting department handles check return item processing appropriately, reconciling all aged items.

2. If the institution offers its customers RDC services, review the appropriateness of:

- Due diligence procedures for new and existing retail customers.
- Due diligence procedures for new and existing third-party processing customers (ensure processors perform adequate due diligence over their originating retail customers).
- Underlying contracts for:
  - Assignment of liability in the event of returned, disputed, or fraudulent items.
  - Limitations or reasonable parameters regarding activity volumes, including returns.
  - Ongoing transaction activity monitoring procedures.

3. Determine whether the institution uses electronic check presentment (ECP) for payment. If yes, determine:

- The effectiveness of the financial institution's ECP implementation, including logical access controls over electronic files storing MICR and related information.
- Whether the financial institution is using positive pay.
- Whether the logical access controls over the electronic files sent by commercial businesses are adequately controlled.

Objective 11: Assess the quality of risk - management of new and emerging technology risks.

1. Determine the institution's processes for evaluating and deploying new and emerging technologies for retail payment systems. Of particular concern are retail payment products and services that do not use established networks such as ACH, or that extend operational processes to the customer location, as with RDC. Determine:

- Whether the institution conducts risk assessments prior to deployment of new and emerging technologies.
- Whether the processes involve the institution's compliance functions, including consumer compliance, BSA/AML, GLBA 501(b), and third party requirements (for example, NACHA, MasterCard, and Visa).
- Whether risk assessment and compliance status are communicated to senior management and the board of directors.

2. Assess the vendor management program over the technology service providers offering new and emerging technologies for retail payment systems. Determine:

- The adequacy of due diligence performed on the technology service provider.
- Whether management regularly reviews the financial status of the technology service provider.
- Whether management receives independent audits, third-party review, or data information security reviews performed on the technology service provider.
- Whether the information exchanged with the technology service provider is documented and meets the bank's requirements.
- Whether the dispute resolution process between the technology service provider and customer is documented and meets the bank's requirements.
- Whether MIS received from the technology service provider is adequate.

CONCLUSIONS

1. Determine the need to conduct Tier II procedures for additional validation to support conclusions related to any of the Tier I objectives.

2. From the procedures performed, including any Tier II procedures performed:

- Document conclusions related to the quality and effectiveness of the management of the retail payment systems function.
- Determine and document to what extent, if any, the examiner may rely upon retail payment system procedures performed by internal or external audit.

3. Review your preliminary conclusions with the examiner-in-charge (EIC) regarding:

- Violations of law, rulings, regulations, and third-party agreements.
- Significant issues warranting inclusion as matters requiring board attention in the report of examination.
- Potential impact of your conclusions on the Uniform Rating System for Information Technology (URSIT) composite and component ratings.
- Where necessary, communicate relevant conclusions to the EIC for the BSA/AML, or retail credit, or compliance examinations.

4. Discuss your findings with management and obtain proposed corrective action, within reasonable timeframes, for significant deficiencies.

5. Document your conclusions in a memo to the EIC providing report-ready comments for all relevant sections of the FFIEC report of examination (ROE) and guidance to future examiners.

6. Organize work papers to ensure clear support for significant findings and conclusions.

TIER II OBJECTIVES AND PROCEDURES

Examination Objective: The Tier II Retail Payment Systems Examination Procedures provide additional validation steps to verify the effectiveness of a financial institution's internal control processes over ACH, EFT/POS network, check item, electronic banking-related retail payments, and bankcard processing, clearance, and settlement. These procedures assist in achieving examination objectives, and examiners may use them in their entirety or selectively, depending upon the scope of the examination and the need for additional verification.

Examiners should coordinate this coverage with other examiners involved in assessing the institution's information systems, operations, information security, business continuity planning, and vendor management effectiveness to avoid duplication of effort and to ensure there is an adequate understanding of the control environment as it pertains to retail payment business lines.

The procedures provided in this section should not be construed as requirements for control implementation. The selection of controls and control implementation should be guided by the risk profile of the institution. Therefore, the controls necessary for any single institution or any given area may differ from those noted in the following procedures.

he Tier II Retail Payment Systems Examination Procedures provide additional validation procedures verifying the effectiveness of a financial institution's internal control processes over ACH processing, EFT/POS network processing, check item processing, electronic banking-related retail payments processing, and bankcard processing, clearance, and settlement. These procedures assist in achieving examination objectives, and examiners may use them in their entirety or selectively. Examiners should coordinate this coverage with other examiners involved in assessing the institution's

information systems, operations, information security, and vendor management effectiveness to ensure there is an adequate understanding of the control environment as it pertains to retail payment business lines and to avoid duplication of effort.

A. EFT/POS and Bankcard Agreements and Contracts

1. If the financial institution is a participant in a shared EFT/POS network or if it contracts with third-party bankcard-issuing or -acquiring processing service providers, determine whether:

- Contracts with regional EFT/POS network switch and gateway operators and bankcard processors clearly set forth the rights and responsibilities of all parties, including the integrity and confidentiality of customer information, ownership of data, settlement terms, contingency and business recovery plans, and requirements for installing and servicing equipment and software.
- Adequate agreements are in place with all technology service providers supplying services for retail EFT/POS and bankcard operations (plastic cards, ATM equipment and software maintenance, ATM cash replenishment) that clearly define the responsibilities of both the service provider and the institution.
- Agreements include a provision of minimum acceptable control standards, the ability of the institution to audit the technology service provider's operations, periodic submission of financial statements to the institution, and contingency and business recovery plans.
- Contracts and agreements clearly define responsibilities and limits of liability for both the customer and financial institution and include provisions of the Electronic Funds Transfer Act (Regulation E) and the Expedited Funds Availability Act (Regulation CC) for deposit activities.

2. Determine whether management periodically reviews individual sites providing retail EFT/POS and bankcard services to ensure policies, procedures, security measures, and equipment maintenance requirements are appropriate.

3. For retail EFT/POS and bankcard transaction processing activities contracted to third-party service providers, assess the adequacy of the review process performed by management regarding annual financial statements, audit reports, and Payment Card Industry (PCI) Data Security Standard assessment.

B. Personal Identification Numbers (PINs)

1. Assess staff access to PIN data. Ensure there is separation of duties between staff responsible for card operations and staff responsible for preparing or issuing bankcards.

2. Assess the adequacy of the PIN generation process. Ensure there is separation of duties between staff responsible for PIN generation and staff responsible for opening accounts or with access to customer account information.

3. For new PIN issuance, assess the adequacy of control procedures including accountability assigned to staff initiating such transactions.

4. Assess the adequacy of PIN generation and issuance procedures to determine whether they preclude matching an assigned PIN to a customer's account number or bankcard.

5. Assess the adequacy of threshold for PIN access attempts to customer account information and funds. The threshold parameter should be set at a reasonable number of unsuccessful attempts.

6. Assess the level of PIN encryption when stored on computer files or transmitted over telecommunication lines.

7. If resets are allowed, assess the adequacy of procedures and controls for PIN/ password resets. The use of single-use and temporary PIN/password is preferred.

8. Assess the adequacy of procedures for prohibiting PIN information from being disclosed over the telephone.

9. Assess staff access to PIN-related databases and determine if management restricts access to authorized personnel. Assess database maintenance activities to ensure management closely supervises and logs staff access.

10. Assess the adequacy of customer PIN selection criteria, focusing on whether the institution discourages or prevents customers from using common words, social security numbers, sequences of numbers, or words or numbers that can easily identify the customer.

C. Information Security

1. Evaluate the logical and physical security controls to ensure the availability and integrity of production retail payment systems applications. Determine:

- Whether the physical and logical security controls established for retail payment transaction processing, clearance, and settlement services maintain transaction confidentiality and integrity.
- Whether physical controls limit access to only those staff assigned responsibility for supporting the operations and business line centers processing retail payment and accounting transactions.
- Whether physical controls provide for the ability to monitor and document access to all retail payment operations facilities.

2. Evaluate the effectiveness of all logical access controls assigned for staff responsible for retail payment-related services. Determine:

- Whether management bases controls on separation-of-duties principles routinely implemented for the processing of financial transactions.
- Whether management bases access controls on a need-to-know basis.

- Whether management bases assigned access to retail payment applications and data on functional staff job duties and requirements.
- Whether identification and authentication schemes include requiring unique logon identifiers with strong password requirements.
- Whether displayed credit and debit card account data are partially masked to prevent full account numbers from being copied.
- Whether network servers are satisfactorily hardened against the risk of internal or external hacking.
- Whether servers simply used for data storage are unnecessarily connected to the Internet.
- Whether sensitive customer information stored electronically is encrypted; if so, at what encryption level.
- Whether internal audit or other third-party have conducted a security review.

3. Evaluate the security procedures for periodic password changes, the encryption of password files, password suppression on terminals, and automatic shutdown of terminals not in use.

4. Assess whether the institution encrypts telecommunications lines used to receive and transmit retail customer and financial institution counterparty data. If not encrypted, evaluate the compensating controls to secure retail payment data in transit. Assess whether any connecting technology service provider's networks used to transport transactions are transporting transaction data in the clear (not encrypted) or use weak forms of encryption.

5. Assess whether merchants use sufficient encryption for wireless sales terminal activity transmitting sensitive customer information.

6. Assess whether customer information being stored is beyond that required by industry standards.

D. Card Issuance

1. Assess bankcard issuance activities, and review control procedures. Determine whether management:

- Issues bankcards only as requested.
- Periodically inventories bankcards.
- Maintains adequate controls for activating new accounts.

2. Assess effectiveness of the dual control procedures for blank card stock in each of the encoding, embossing, and mailing steps.

3. Assess adequacy of physical access controls for card encoding areas. Management should allow access to authorized personnel only.

4. Assess whether inventory controls for plastic card stock make them physically secure.

5. Assess whether management restricts the use of bankcard encoding equipment to authorized personnel only.

6. Assess adequacy of procedures for issuing cards from more than one location (e.g., branches) to ensure there are accountability and bankcard control procedures at each card-issuing location.

7. Assess adequacy of institution card-mailing procedures. Ensure the institution mails the card and associated PIN to customers in separate envelopes. Also ensure that the return address does not identify the institution.

8. Assess whether mailing procedures provide for a sufficient time between the card and PIN mailings.

9. Assess adequacy of returned card procedures. Determine whether adequate controls are in place to ensure returned cards are not sent to staff with access to, or responsibility for, issuing cards.

10. Assess whether there is appropriate follow-up to determine whether the correct customer received the card and PIN.

11. Assess the adequacy of control procedures (e.g., hot card lists and expiration dates) to limit the period of exposure if a card is lost, stolen, or purposely misused.

12. Determine whether the institution destroys captured and spoiled cards under dual control and maintains records of all destroyed cards.

13. Assess whether the institution adequately controls test or demonstration cards.

14. Assess whether management maintains satisfactory controls over the issuance of replacement or additional cards to the customer (e.g., temporary access cards issued to the customer).

15. Assess the adequacy of the vendor management program to determine whether the institution reviews card issuance services contracted to third parties for compliance with appropriate bankcard control procedures.

E. Business Continuity Planning

1. Assess the adequacy of the financial institution's business continuity plans for a partial or complete failure of each retail payment system. Determine whether the plans include:

- Recovery of all required components linking the institution with third-party network switch, gateway, or related third-party data centers and bankcard processors.
- Information relative to the volume and importance of the retail payment system activity to the institution's overall operation.
- Provisions for acceptable store and forward procedures to protect against loss or

duplication of data and to ensure full recovery within reasonable timeframes.

- Provisions for secured transport and off-site storage of sensitive customer information.
- Stand-in arrangements with other financial institutions, allowing for interim bankcard processing in the event of an outage.
- Adequate testing of plans accounting for various recovery scenarios.

F. EFT/POS and Bankcard Accounting and Transaction Processing

1. Assess the adequacy of reconciliation processes for general ledger accounts related to bankcard and debit card transaction processing activity. Determine whether:

- Accounting reconciles bankcard and ATM transaction activities daily.
- Retail payment system supervisory personnel periodically review reconcilement and exception item reports.
- Accounting periodically reconciles accounts used to control rejects, adjustments, and unposted items.

2. Assess the adequacy of the daily settlement process for institutions participating in shared EFT/POS networks or gateway systems.

3. Assess the adequacy of transaction reconstruction procedures. Transaction files should be duplicated or otherwise retained for a minimum of 60 days, as required by Regulation E, in order to identify unauthorized transactions.

4. Assess the adequacy of the investigative unit in place to address customer inquiries and control non-posted items, rejects, and differences. Management should periodically receive aging reports that list outstanding items.

5. Assess the adequacy of separation of duties for the bankcard and EFT/POS account posting process including receipt of transactions, file updates, adjustments, internal reconcilement, preparation of general ledger entries, posting to customers accounts, investigations, and reconcilement with third-party service provider network switches and card processors.

6. Assess the effectiveness and accuracy of the adjustment process (e.g., changes to deposits and reversals) relating to retail EFT/POS and bankcard transactions processed by staff.

7. For institutions involved in bankcard issuing or acquiring services, determine whether the institution has established:

- Proper accounting controls for the balancing, settling, and reconciliation of all bankcard and acquiring accounts under its control.

- Appropriate credit and liquidity risk measures for the bankcard and acquiring business lines.
- Appropriate controls for the processing of customer or merchant transaction flows.

G. EFT/POS Operational Controls

1. Assess the effectiveness of personnel responsible for internal ATM processing. Determine whether there are:

- Controls prohibiting staff members who originate entries from processing and physically handling cash.
- Proper control of all source documents (e.g., checks for deposit) maintained throughout the daily processing cycle relative to:
  - Input preparation,
  - Reconcilement of item counts and totals,
  - Output distribution, and
  - Storage of the instruments.

2. Determine whether terminal and operator identification codes are used for all retail ATM and POS transactions.

3. Assess the adequacy of controls in place to prevent customer charges from exceeding the available balance in the account or approved overdraft lines.

4. Assess the adequacy of access controls for terminals used to change customer credit lines and account information.

5. Determine whether retail EFT equipment keyboards or display units are properly shielded to avoid disclosure of customer IDs or PINs.

6. Determine whether receipt issuance ensures customers receive a receipt showing the amount, date, time, and location for retail EFT transactions in compliance with Regulation E.

7. Assess whether each retail EFT transaction is assigned a sequence number and terminal ID to provide an audit trail.

8. Assess whether the institution regularly updates hot card or customer suspect lists and distributes them to branch banking locations.

9. Assess the adequacy of verification procedures for telephone-initiated payments or transfers and ensure confirmations are promptly sent to customers and merchants.

10. Assess the adequacy of security devices and access control procedures for EFT/

POS, bankcard, and acquiring processing facilities to ensure appropriate physical and logical access controls are in place.

H. ACH ODFI and RDFI Responsibilities

1. Determine whether agreements between the ODFI and originators adequately address

- Liabilities and warranties,
- Responsibilities for processing arrangements, and
- Other originator obligations such as security and audit requirements.

2. Determine whether the ODFI has established procedures to monitor the creditworthiness of its originator customers on an ongoing basis. Determine whether:

- The ODFI assigns credit ratings to originators.
- Competent credit personnel perform monitoring, independent of ACH operations.
- Written agreements with originators require the submission of periodic financial information.

3. Determine whether the ODFI has established ACH exposure limits for originators. Determine whether:

- The limit is based on the originator's credit rating and activity levels.
- The limit is reasonable relative to the originator's exposure across all services (lending, cash management, foreign exchange, etc.).
- Limits have been established for originators whose entries are transmitted to the ACH operator by a technology service provider.
- Written agreements with originators address exposure limits.
- A separate limit for WEB entries and other high-risk ACH transactions, as warranted, has been established.

4. Determine whether the ODFI reviews exposure limits periodically. Determine whether:

- The ODFI adjusts limits for changes in an originator's credit rating and activity levels.

- Increases in an originator's ACH debit return volume trigger a re-evaluation of the exposure limit.
- The ODFI reviews the limits in conjunction with the review of an originator's exposure limit across all services.

5. Determine whether the ODFI has implemented procedures to monitor ACH entries initiated by an originator relative to its exposure limit across multiple settlement dates. Determine whether:

- The monitoring system is automated and accumulates entries for a period at least as long as the average ACH debits return time (60-75 days).
- Entries in excess of the exposure limit receive prior approval from a credit officer.
- WEB entries and other high-risk ACH transactions (as warranted) are accumulated and monitored separately, yet integrated into the overall ACH transaction monitoring system.

6. Assess the RDFI's overdraft and funds availability policies and practices and determine whether they adequately mitigate its credit exposures to ACH transactions.

7. Determine the adequacy of the ODFI's practices regarding originators' annual or more frequent security audits of physical, logical, and network security. Determine whether:

- The ODFI receives summaries or full audit reports from the originators.
- The audits are adequate in scope and performed by independent and qualified personnel.
- Corrective actions regarding exceptions are satisfactory.

8. Determine how the ODFI or RDFI manages its relationship with technology service providers. Determine whether:

- The service provider's financial information is obtained and satisfactorily analyzed.
- Service-level agreements are established and monitored.

9. Determine whether the ODFI allows technology service providers direct access to an ACH operator. Consider whether agreements between the ODFI and the service providers include:

- A requirement that the service provider obtain the prior approval of the ODFI before originating ACH transactions for originators under the ODFI routing number.
- The establishment by the ODFI of dollar limits for files that the service provider deposits with the ACH operator.
- A provision that restricts the service provider's ability to initiate corrections to files that have already been transmitted to the ACH operator.
- Provisions regarding warranty and liability responsibilities.
- Appropriate handling of files (physical and logical access controls).

10. Determine whether the RDFI has established procedures to deal with consumers' notifications regarding unauthorized or improperly originated entries or entries where authorization was revoked.

11. Determine whether the RDFI acts promptly on consumers' stop-payment orders.

12. Determine whether the RDFI has procedures that enable it to freeze proceeds of ACH transactions in favor of blocked parties (under OFAC sanctions) for whom the RDFI holds an account.

13. Determine whether the financial institution considers the volume of its uncollected ACH transactions as part of its liquidity risk management practices.

14. Determine whether management and personnel display adequate knowledge and technical skills in managing and performing duties related to ACH transactions.

15. Review results from the financial institution's NACHA rule compliance audit. Determine:

- The independence and competence of the party performing the audit.
- Whether the board or its committee reviewed and approved the audit.
- Whether responsibilities for high-risk entries, such as WEB, were included in the scope.
- Whether corrective actions on audit exceptions are satisfactory.

I. ACH Accounting and Transaction Processing

1. Assess the adequacy of logs maintained for ACH payments received from, and delivered to, each customer.

2. Assess the adequacy of the balancing procedures used for all ACH payments received and whether they include balancing to the aggregate payments sent to an ACH operator.

3. Determine whether the institution balances all payments received from an ACH operator to the aggregate of payments delivered to customers.

4. Determine whether the institution verifies and authorizes the source of all ACH files received for processing.

5. Determine whether the institution reconciles all general ledger accounts related to ACH activities on a timely basis.

6. Determine whether ACH supervisory personnel perform reconcilement and regularly review exception items.

7. Determine whether the institution reconciles the ACH activity and pending file totals daily with the ACH operator.

8. Assess the effectiveness of the reconcilement with third-party service providers preparing ACH transaction files and ensure daily reconciliation.

9. Assess the effectiveness of ACH holdover transactions and determine whether the institution adequately controls them.

10. Determine whether accounting staff reconciles individual outgoing ACH batches before merging them with other ACH transactions.

11. Determine whether there are separate accounts to control holdovers, adjustments, return items, rejects, etc. and whether they are periodically reconciled.

12. Assess the effectiveness of the investigation unit to address customer inquiries and control return items, rejected/unposted items, differences, etc. Determine whether the unit periodically generates aging reports of outstanding items for management.

13. Assess whether management adequately tracks exceptions to credit limit policies and legal contracts.

14. Determine whether exception reports (e.g., rejects, return items, and aging of open items) receive appropriate management attention.

15. Assess the adequacy of separation of duties throughout the ACH process including origination, data entry, adjustments, internal reconcilement, preparing general ledger entries, posting to customer accounts, investigations, and reconcilement with ACH operators.

16. Determine whether adjustments (e.g., added payments, stop payments, reroutes, and reversals) to original ACH instructions are received in an area that does not have access to the original data files.

17. Assess whether controls are appropriate for the adjustment process, including authorization (e.g., signature verification and callbacks on telephone instructions) and whether the institution maintains adequate records (e.g., logs and taping of telephone calls) of individuals making requests.

18. Determine the adequacy of the customer profile origination and change request process. Consider whether requests:

- Are in writing or equivalent confirmation for online activities.
- Identify the originating personnel.
- Document supervisory approval.
- Are verified by staff unable to make changes.

J. ACH Funding and Credit

1. Assess the adequacy of the process for releasing payments to an ACH operator, and determine whether assurances are obtained that sufficient collected funds (e.g., on deposit or prefunded) or credit facilities are available. The institution should monitor customer intraday and interday positions based on defined thresholds.

2. For third-party service providers contracted to process outgoing ACH transactions, determine whether there are procedures to monitor ACH activity and ensure that funds are collected (collected balances, prefunding, credit lines) before the institution settles with the ACH operator.

3. For prefunding arrangements in place for customers without credit lines, determine whether management blocks funds (held for disposition) or maintains them in separate accounts until the transaction date.

4. For non prefunded arrangements determine whether the institution places blocks on outgoing payments to deposit accounts, applies them as reductions to credit lines, or includes them in the overall funds transfer monitoring process.

5. Determine whether management approves payments resulting in extensions of credit lines or drawings against uncollected funds and retains documentation to support the approvals. Determine whether the institution performs credit assessments of customers originating large dollar volumes of ACH credit transactions. Credit assessments should also be reviewed periodically to evaluate creditworthiness of the customer and current economic conditions.

6. Determine whether management treats ACH debits deposited as uncollected funds and whether they monitor any draws against these funds for debits originated by high-risk customers.

7. Determine whether management approves draws against uncollected ACH deposits and maintains documentation to support approvals for debits originated by high-risk customers.

8. Determine the adequacy of Internet and telephone ACH transaction processing procedures and determine whether there are appropriate authentication controls and procedures to ensure the proper identities of parties invoking ACH transactions.

9. Assess the adequacy of management's risk assessment of ACH services in terms of the importance of this function to the overall corporate treasury services function.

10. Ensure that the financial institution obtains and analyzes all audits conducted by the ACH service provider, pursuant to the NACHA rule compliance audit requirement.

K. Web and Telephone-Initiated ACH Transactions

1. Determine whether the financial institution has adopted adequate policies and procedures regarding ACH transactions involving Internet-initiated (WEB) entries. Determine whether they:

- Are in writing and approved by the board or a designated committee.
- Adequately address ODFI or RDFI responsibilities.
- Establish management accountability.
- Include a process to monitor policy compliance.
- Include a mechanism for periodic reviews and updates.

2. Determine whether the ODFI has implemented telephone-initiated (TEL) ACH entries. Determine whether:

- There are significant return rates for these transactions.
- The institution adheres to NACHA guidelines concerning merchant management and their business practices.
- Written agreements are in place with all originators submitting TEL transactions, and include adequate consumer (receiver) authentication and authorization.
- The institution makes tape recordings of all consumer oral authorizations.
- The institution provides written notice to the consumer, prior to settlement date for the TEL entry, confirming the terms of the oral authorization.

3. Determine whether the ODFI requires its originator to employ a commercially reasonable method to authenticate the consumer/business. Determine whether:

- Documentation of the method is adequate.
- The frequency of the review of commercially reasonable standards is sufficient.

4. Determine whether the ODFI conducts risk assessments of its originators and whether they reflect a reasonable exercise of business judgment. Consider whether the risk assessment includes evaluations of:

- Receiver authorizations.
- Originator's Internet security capability, including;
  - Commercially reasonable fraudulent transaction detection systems and routing number verification,
  - Secure customer Internet sessions, and
  - Annual (or more frequent) security audits based on risk.
  - Frequency of risk assessments.
  - Documentation and approval standards.

L. ACH Contingency Plans

1. Evaluate the adequacy of the ACH contingency plan; determine whether the financial institution has tested it and whether it includes provisions for partial or complete failure of the system or communication lines between the institution, ACH operators, customers, and associated data centers.

2. Based on the volume and importance of ACH activity, evaluate whether the plan is reasonable and whether it provides for a reasonable recovery period.

3. Determine whether the institution duplicates or retains transaction files for input reconstruction for a minimum of 24 hours. Note that NACHA rules require the retention of all entries, including return and adjustment entries, transmitted to and received from the ACH for a period of six years after the date of transmittal.

4. Determine whether data and program files are adequately secured, retained, and backed up at off-premises facilities, including secured transport mechanisms for those resources.

5. Determine whether the center has established and tested procedures to recover and restore data under various contingency scenarios.

6. Determine whether the frequency and methods of testing contingency plans are adequate.

M. Check 21

(A more comprehensive set of examination procedures that are designed to test transactions can be found at the FFIEC Check 21 InfoBase at www.ffiec.gov/exam/check21/default.htm.)

1. Determine whether:

- The institution manages check return items effectively and whether there are significant numbers of return items.
- The institution records source-document images for recovery if the originals are lost

in transit.

- The institution reconciles batch-dollar totals after processing.
- Reject items are properly segregated from other work.
- Exception items are controlled and tracked adequately.
- Item processing duties are segregated appropriately.

2. If a financial institution has begun to image checks or retrieve imaged checks pursuant to Check 21, determine whether the institution has the following:

- Consumer awareness program.
- Customer service - training and education process.
- Procedures for expedited re-credit.
- Procedures to qualify returns of substitute checks.
- Procedures to identify duplicate checks.
- Procedures for statement preparation and processing.
- Procedures for item repair.
- Procedures for managing corporate customers wanting to submit substitute checks.

3. If the financial institution is a reconverting institution pursuant to Check 21, determine whether it has the following:

- Procedures to identify, measure, and monitor fraud risk.
- Security features for substitute checks.
- Procedures for retention and retrieval of original items.
- Procedures for identifying/controlling duplicate checks.
- Procedures or processes to control substitute check shrinkage.
- Procedures and processes to manage quality.
- Procedures and processes to manage endorsements (includes electronic).
- Procedures and processes to manage re-presentments.
- Procedures to ensure full MICR line is on all substitute checks.

- Procedures and processes to control cash letters.

4. If the financial institution accepts RCCs from retail business customers or payment processing customers, assess the appropriateness of, and adherence to, policies and procedures regarding customer due diligence, customer contracts, third-party service provider's due diligence, and activity/transaction monitoring. Consider the following elements relative to the institution's retail customers, its payment processing customers, and any processors' retail customers:

- Customer due diligence performed at the initiation and periodically throughout the business relationship, including;
  - Assessment of risk exposure associated with the customer's underlying business models;
  - Review of operational history of customer (e.g., length of time in business, relocations of operations, and business reputation);
  - Performance of background checks on customer's principals and/or key operators.
  - Execution of contracts with customers containing provisions addressing;
    - Customer's agreement to operate in accordance with applicable laws and regulations (i.e., FTC Telemarketing Rule, UCC provisions);
    - The parties' responsibilities and warrants under Regulation CC;
    - Customer activity and/or transaction parameters and limits, including expected/allowable unauthorized return levels;
    - Auditing and/or access rights to customers' marketing scripts and consumer authorization/verification files;
    - The financial institution's ability to terminate the business relationship.
  - Routine monitoring and reporting of customer activity and transaction levels, including:
    - The integrity and timeliness of MIS reports on individual and aggregate customer activity/transaction and exposure levels;
    - Established management accountability throughout the business line, including an established process to report monitoring conclusions and exceptions to executive management;
    - Periodic re-assessment of customer exposure and/or transaction limits in association with customer due diligence and contract reviews;
    - The application of independent quality assurance or internal audit reviews to customer relationships in general and to customer monitoring activities in particular;

- Performance of on-site verification of customer authorization files where warranted.

N. Remote Deposit Capture Risk Management

1. Identify the key elements of the RDC environment.

- Identify the bank staff, customers, and technology service providers (if applicable) involved in the RDC function. Obtain and review reports of RDC volume (number of transactions and dollar ranges) for the financial institution as a whole and for individual customers.
- Obtain and review the topology of the financial institution's network, and determine the components involved in the RDC process. Identify the network interfaces with customers using RDC and the technology controls in place.
- Obtain and review the financial institution's data flow or process flow diagram, including relationships with any third-party service providers (if applicable) and the relationships with RDC customers. Identify when the diagram was last updated, and assess whether it is consistent with the system currently implemented.
- Identify whether the RDC system has the following features or functionality:
  - Duplicate item detection.
  - Scanner options (simplex/duplex, MICR/OCR, franking/spraying, CAR/LAR, etc.).
  - Interoperability with existing systems and/or ancillary applications (e.g., QuickBooks).
  - MIS and reporting (audit logs, activity reports).
  - Image quality.
  - Ability to change routing number, account number, and amount.
  - Least-cost routing functionality (conversion into different payment stream).
  - ABA validations (to identify deposits drawn on US versus foreign financial institution).
  - Ability to integrate with BSA/AML systems and processes.
  - Ability to integrate with OFAC systems.
  - Integration with enterprise-wide BCP.
  - Information security (authentication, access controls, encryption, etc.).

2. Assess the RDC strategic planning and the risk assessment process.

- Obtain and review the financial institution's strategic plan for the implementation of RDC.
- Review board or board committee minutes involving discussion and approval of RDC implementation. Note the date of approval.
- Summarize the key objectives of the strategic plan, including:
  - The rationale for offering RDC (e.g., maintaining existing customers or attracting new customers; maintaining existing geographic footprint or penetrating new market/geographic area; wholesale only [merchant/commercial] or retail [consumer]).
  - The type of RDC to be offered (e.g., thick vs. thin client) or if multiple types will be offered to a single client.
  - The use of technology service providers.
  - Other key objectives.
  - Describe the risk assessment process. Identify the financial institution's participants (e.g., representation from such functions as credit, IT, compliance, deposit operations, internal audit, and legal).
  - Obtain and review the most recent risk assessment related to RDC. Evaluate the quality of the risk assessment and whether it encompasses factors such as:
    - Scope of product implementation.
    - Type of customer (e.g., commercial, retail, foreign correspondent).
    - Type of cash letter instrument and the geographic location of the originator.
    - Financial institution position in payment process and settlement channels used (bank of first deposit vs. nonbank of first deposit).
    - Current and anticipated volume of RDC transactions (number and dollar amounts of transactions).
    - Customer role and responsibility in the RDC process.
    - Customer ability to download and retain nonpublic information (NPI).
    - Financial institution's approved technology service providers and equipment.
    - Clearing and settlement channels: image exchange, ACH, or both.
    - Ability to integrate RDC into:
      - Anti-money laundering systems and processes.
      - BCP.

- Information security planning.
- Staffing and customer support.
- Determine whether the RDC risk assessment is updated on a periodic basis as technology, market, customer base, industry, or processes change. Identify the date of the last risk assessment or update.

3. Customer due diligence and suitability.

- Describe the process, the financial institution staff involved, and the decision criteria the financial institution uses to conduct a due diligence review to qualify potential customers for the RDC delivery system. Consider the following:
  - The function and level of the financial institution's staff who conduct the due diligence, and those who have the authority to approve a customer for RDC;
  - How the financial institution risk rates existing customers, on a recurring basis, and how they qualify potential customers;
  - The information the financial institution reviews for potential customers such as:
    - Customer application.
    - Financial analysis.
    - Years in business (for commercial customers).
    - Loan/deposit history.
    - Credit score.
    - Business practices.
    - Sufficiency of staff.
    - Compliance with PCI standards (when appropriate).
    - Publicly available reports for customers that are companies (e.g., Dun & Bradstreet).
    - Visa/MasterCard terminated merchant file or ChexSystems reports, when appropriate to the customer
    - Whether the financial institution has procedures that address customer identification as explained in the BSA/AML manual.
    - Whether the financial institution has procedures to address foreign correspondent relationships and international cash letter pouch activity as explained in the BSA/AML manual.
  - Describe the process and criteria used by financial institution management to

evaluate the RDC customers' information security infrastructure and risk management processes.

4. Vendor Management

- Where technology service providers are used, determine whether RDC is included in the institution's vendor management program.
- Describe any service-level agreements between the financial institution and its service providers, and determine whether management of these relationships conforms to the Outsourcing Technology Services booklet.
- Determine whether any of the financial institution's RDC customers use a service provider in the RDC process. If so, evaluate how the financial institution manages risks, and whether the process is adequate.

5. Contracts and Agreements

- Determine whether legal counsel was involved in drafting any RDC-related contracts or agreements with technology service providers or customers.
- Obtain and review a sample contract or agreement between the financial institution and the RDC customer and technology service provider, where applicable. Consider whether contracts or agreements address the following:
  - Governing laws, regulations, guidelines, payment system rules, and other operational considerations relevant to traditional deposit processing.
  - Roles, responsibilities, and performance standards of the parties, including those related to the sale or lease of equipment needed for RDC at the customer location.
  - Liabilities, warranties, and indemnifications of all parties.
  - Types of items that may be transmitted.
  - Processes and procedures that the customer must follow (e.g., image quality).
  - Funds availability, collateral, collected funds, and reject/return requirements.
  - System maintenance and administration guidelines (e.g., change control and logical access administration).
  - Dispute resolution.
  - Information security requirements and procedures.
  - Security incident reporting.

- Customer service and technical support.
- Responsibility for network connectivity.
- Establishment of controls, such as deposit limits, overdraft limits, and payment on uncollected funds.
- Retention requirements and physical and logical security over deposit items and electronic files at the RDC customer location.
- Business continuity planning requirements, including the back-up of data and periodic testing of such plans.
- Limiting high-risk customers to one account for RDC.
- Authority of the financial institution to mandate specific internal controls at the customer's location(s); audits of customer operations; and requests for additional customer information, as necessary.
- Authority of the financial institution to terminate the RDC relationship.

6. Insurance

- Determine whether financial institution management assessed the availability, coverage, and suitability of insurance related to RDC. If coverage has been obtained, describe.

7. Physical and Logical Access Controls

- Describe how financial institution management ensures that appropriate physical security controls exist at the RDC customer location, such as:
  - Building security.
  - Check storage.
  - Ensuring appropriate controls over portable RDC-related equipment, such as computers and scanner equipment and software.
  - Transport mechanisms for moving data to off-site storage locations.
  - Describe how financial institution management ensures that appropriate logical security controls exist at the RDC customer location, such as:
    - Encrypted data transmission and storage.
    - Multifactor or other strong authentication.
    - Access level controls.

- Password security parameters.
- Equipment enrollment.

8. Separation of Duties

- Describe how financial institution management has established appropriate separation of duties for the system administration and security monitoring functions. For example, does one person assign users or rights and another review the activity reports?
- Describe how the financial institution and its RDC customers have implemented appropriate separation of duties controls over the remote capture and transmission process.
- Determine whether the financial institution performs any data entry functions (e.g., adjusting dollar amounts), and whether there is an independent review or reconciliation.
- Determine whether the financial institution requires separation of duties at the RDC customer location and how it monitors for compliance. If separation of duties is not mandatory or possible, describe any required compensating controls required at the RDC customer location.

9. Oversight and Monitoring

- Obtain and review the financial institution's policies and procedures for RDC. Assess whether they define the function, responsibilities, operational controls, vendor management, customer due diligence, BSA/AML compliance monitoring, and reporting functions, etc. Identify the date they were last reviewed and approved by the board or a board committee.
- Identify the financial institution staff members who perform periodic monitoring of RDC customer activity and describe the process used.
- Determine the frequency and process for management review of logical and physical access privileges and audit trails/logs.
- Identify and describe the monitoring reports used by the financial institution to manage risk. Obtain copies of reports used and review the monitoring process with appropriate financial institution staff. Discuss with appropriate financial institution staff the internal processes for responding to established threshold breaches and any escalation process. Examples include:
  - Duplicate Presentment Report (to detect duplicate batches prior to submission);
  - Daily Batch Totals Report;

- Velocity Exception Report (to detect merchant spikes in volume or exceeding approved dollar limits);
- Large Item Report (exception report to detect whether transactions are outside of normal parameters); and,
- Customer Activity Report (detailed log of activity by merchant, including batch delivery date, time, value, receipt acknowledgement, and merchant operator ID).
- Identify and describe the RDC customer risk management reports recommended by financial institution management. Discuss how financial institution management validates that RDC customers review the reports. Examples include:
  - Pending Batch Report (items queued for processing for reasonableness and timeliness reviews);
  - Batch Total Report (allows the merchant to reconcile processed RDC work to the batch prepped for submission to the FI);
  - Return Item Report (alerts management to operational deficiencies, e.g., poor image quality);
  - Duplicate Presentment Report (to detect duplicate batches prior to submissions); and,
  - FI Reports (report would provide list of received imaged items).
- Select a sample of RDC customers and review the nature of account activity relative to the business type.

10. Training

- Determine whether financial institution management has established a training program to ensure that all parties involved are trained appropriately. If yes, describe the training programs for financial institution and customer staff.
- Determine whether the financial institution provides or plans to provide customer technical service or support to the RDC customers. If yes, discuss whether the financial institution considered the need for, or has added, additional staff.
- Determine whether the financial institution provides the merchant/consumer customers with a procedural or instructional document and a user guide for the application/scanner.

11. Change Management

- Determine whether the financial institution has enhanced its change management program to address the procedures involved in the RDC function and ensure ongoing compatibility between financial institution and customer systems. Describe the coordination process.
- If the financial institution maintains the application in-house, describe how it ensures that all relevant operating system and application patches are up-to-date.
- Describe how financial institution management ensures that RDC customers implement an effective change management program to maintain updated and patched network and desktop operating systems, RDC application, anti-virus, etc.

12. Records Management

Assess the process by which financial institution management verifies customer compliance with contract requirements related to the secure retention, storage, and destruction requirements for physical deposit items and electronic files.

13. Business Continuity Planning (BCP)

- Determine whether the financial institution's BCP has been updated to address:
  - The financial institution's relationship with the RDC service provider and BCP assurance.
  - The financial institution's relationship with the RDC customer.
  - Determine whether the financial institution's BCP testing activities include:
    - RDC systems and processes.
    - RDC customers.
    - Technology service providers, where appropriate.

14. Fraud

- Describe how financial institution management monitors for fraud associated with RDC.
- Describe how the financial institution attempts to mitigate fraud risks (e.g., duplicate check detection, establishing deposit limits, safeguarding checks).
- Describe how the financial institution monitors items that originated in foreign countries (i.e., foreign locations owned or controlled by customers of the financial institution or items received and processed by correspondent banks).

O. Vendor Management

Assess the adequacy of vendor management program over a service provider that provides a new and emerging retail payment technology. (Select one or more projects involving the development and deployment of a new and emerging retail payment technology and complete the following procedures.)

1. Review documentation supporting the business case for the application

- Scope and nature;
- Standards for controls;
- Minimum acceptable service provider characteristics;
- Monitoring and reporting;
- Transition requirements;
- Contract duration, termination, and assignment; and
- Contractual protections against liability.

2. Assess the extent to which the institution

- Reviews the financial stability of the technology service provider;
- Analyzes the service provider's audited financial statements and annual reports;
- Assesses the service provider's length of operation and market share;
- Considers the size of the institution's contract in relation to the size of the service provider;
- Reviews the service provider's level of technological expenditures to ensure on-going support; and
- Assesses the impact of economic, political, or environmental risk on the service provider's financial stability.

3. Evaluate whether the institution's due diligence considers the following:

- References from current users or user groups about a particular technology service provider's reputation and performance;
- The service provider's experience and ability in the industry;

- The service provider's experience and ability in dealing with situations similar to the institution's environment and operations;
- The cost for additional system and data conversions or interfaces presented by the various technology service providers;
- Shortcomings in the service provider's expertise that the institution would need to supplement in order to fully mitigate risks;
- The service provider's proposed use of third parties, subcontractors, or partners to support the outsourced activities;
- The service provider's ability to respond to service disruptions;
- Key service provider personnel that would be assigned to support the financial institution;
- The service provider's ability to comply with appropriate federal and state laws. In particular, ensure management has assessed the service providers' ability to comply with federal laws (including GLBA and BSA); and
- Country, state, or local risk.

4. Verify that the contract appropriately addresses:

- Scope of services;
- Performance standards;
- Pricing;
- Controls;
- Financial and control reporting;
- Right to audit;
- Ownership of data and programs;
- Confidentiality and security;
- Regulatory compliance;
- Indemnification;
- Limitation of liability;
- Dispute resolution;
- Contract duration;
- Restrictions on, or prior approval for, subcontractors;

- Termination and assignment, including timely return of data in a machine-readable format;
- Insurance coverage;
- Prevailing jurisdiction (where applicable);
- Choice of Law (foreign outsourcing arrangements);
- Regulatory access to data and information necessary for supervision; and
- Business Continuity Planning.

5. Review service level agreements to ensure they are adequate and measurable. Determine whether:

- Significant elements of the service are identified and based on the institution's requirements;
- Objective measurements for each significant element are defined;
- Reporting of measurements is required;
- Measurements specify what constitutes inadequate performance; and
- Inadequate performance is met with appropriate sanctions, such as reduction in contract fees or contract termination.

6. Evaluate the institution's periodic monitoring of the service provider relationship(s), including:

- Timeliness of review, given the risk from the relationship;
- Changes in the risk due to the function outsourced;
- Changing circumstances at the service provider, including financial and control environment changes;
- Conformance with the contract, including the service level agreement; and
- Audit reports and other required reporting addressing business continuity, security, and other facets of the outsourcing relationship.

Appendix B: Glossary

CHIPS - A private-sector U.S.-dollar funds transfer system, clearing and settling cross-border and domestic payments.

Debit card - A payment card issued as either a PIN-based debit (ATM) card or as a signature-based debit card from one of the bankcard associations. A payment card issued to a person for purchasing goods and services through an electronic transfer of funds from a demand deposit account rather than using cash, checks, or drafts at the point-of-sale.

Debit entry - An entry to the record of an account to represent the transfer or removal of funds from the account.

Deferred net settlement - See "National Settlement Service".

Depository - An institution that holds funds or marketable securities for safekeeping. Depositories may be privately or publicly operated and allow securities transfers through book-entry and offer funds accounts permitting funds transfers as a means of payment.

Depository bank (Check 21) - Also known as Bank of First Deposit (BOFD). The first bank to which a check is transferred even though it is also the paying bank or the payee. A check deposited in an account is deemed to be transferred to the financial institution holding the account into which the check is deposited, even though the check is physically received and endorsed first by another financial institution.

Direct debit - Electronic transfer, usually through ACH, out of an individual's checking (or savings) account to pay bills, such as mortgage payments, insurance premiums, and utility payments. Also referred to as “direct payment.”

Direct deposit - Electronic deposits or credit, usually through ACH, to an individual’s deposit account. Common uses of direct deposit include payroll payments, Social Security benefits, and income from investments such as CDs, annuities, and mutual funds.

Direct presentment - Depositary banks can present checks directly to the paying institution. The paying institution may be the depositary bank (no settlement is needed), or, if not, may settle on the books of the Federal Reserve, using the Federal Reserve’s national settlement service.

Electronic Benefits Transfer (EBT) - A type of EFT system involving the transfer of public entitlement payments, such as welfare or food stamps, through direct deposit or point-of-sale technology (see POS). The recipient can be given an identification card, similar to a benefit card, and a PIN allowing access to the benefits through an electronic network.

Electronic bill presentment and payment (EBPP) - An electronic alternative to traditional bill payment, allowing a merchant or utility to present its customers with an electronic bill and the payer to pay the bill electronically. EBPP systems usually fall within two models: direct and consolidation-aggregation. In the direct model, the merchant or utility generates an electronic version of the consumer’s billing information, and notifies the consumer of a pending bill, generally via e-mail. The consumer can initiate payment of the electronically presented bill using a variety of payment mechanisms, typically a credit card. In the consolidation-aggregation model, the consumer’s bills are consolidated by a

consolidator acting on behalf of merchants and utilities (or aggregated on behalf of the consumer), combining data from multiple bills and presenting a single source for the consumer to initiate payment. Some consolidators present bills at their own web sites, typically most support the aggregation of bills by consumer service providers such an Internet portals, financial institutions, and brokerage web sites.

Electronic check conversion - The process by which a check is used as a source of information for the check number, the customer's account number, and the number that identifies the financial institution. The information is used to make a one-time electronic payment from the customer's account -- an electronic fund transfer. The check itself is not the method of payment.

Electronic check presentment (ECP) - Check truncation methodology in which the paper check's MICR line information is captured and stored electronically for presentment. The physical checks may or may not be presented after the electronic files are delivered, depending on the type of ECP service that is used.

Electronic commerce (E-Commerce) - A broad term encompassing the remote procurement and payment by businesses or consumers of goods and services through electronic systems such as the Internet.

Electronic data capture (EDC) - Process used for capturing and transferring the encoded information on the magnetic strip from a bankcard or debit card at the point-of-sale to the processor's database.

Electronic funds transfer (EFT) - A generic term describing any transfer of funds between parties or depository institutions through electronic data systems.

Electronically-created payment orders - These are payment orders received by merchants from consumers, typically by telephone or the Internet. These payment orders are processed through the check processing system although they were not initiated as paper checks. These payment orders are not subject to check law and are not warranted by the Federal Reserve Banks.

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.

Expedited Funds Availability Act (EFAA) - See "Regulation CC".

Federal Reserve Banks - The Federal Reserve Banks provide a variety of financial services including retail and wholesale payments. The Federal Reserve Bank operates a nationwide system for clearing and settling checks drawn on depository institutions located in all regions of the United States.

Fedwire® - The Federal Reserve Bank's nationwide real time gross settlement electronic funds and securities transfer network. Fedwire® is a credit transfer system. Each funds transfer is settled individually against an institution's reserve or clearing account on the books of the Federal Reserve. The transaction is considered an irrevocable payment as it is processed.

Finality - Irrevocable and unconditional transfer of payment during settlement.

Financial EDI (FEDI) - Financial electronic data interchange. An instrument for settling invoices by initiating payments, processing remittance data and automating

reconciliation, through the exchange of electronic messages.

Float - Funds held by an institution during the check-clearing process before being made available to a depositor. Interest may be earned on these funds.

Gramm-Leach-Bliley Act (GLBA) - The GLBA, also known as the Financial Services Modernization Act of 1999, (Pub.L. 106-102, 113 Stat. 1338, enacted November 12, 1999), required the Federal banking agencies to establish information security standards for financial institutions.

Image archive (Check 21) - Database for storage and easy retrieval of check images.

Image capture (Check 21) - The process of digitizing both sides of physical items and their assorted MICR information as they are processed at the Federal Reserve Bank. Also includes storage of the images for up to 60 days.

Image exchange (Check 21) - Exchange of some or all of the digitized images of a check.

Indemnifying bank (Check 21) - A financial institution that transfers, presents, or returns a substitute check or a paper or electronic representation of a substitute check for which it receives consideration. The financial institution shall indemnify the recipient and any subsequent recipient (including a collecting or returning financial institution, the depository financial institution, the drawer, the drawee, the payee, the depositor, and any endorser) for any loss incurred by any recipient of a substitute check if that loss occurred due to the receipt of a substitute check instead of the original.

Interbank checks - Checks that are not “on-us.” They are cleared and settled either by direct presentment, a clearinghouse association, a correspondent bank, or a Federal Reserve Bank.

Interchange - Exchange of transactions between financial institutions participating in a bank card network, based on a common set of rules. Card interchange allows a financial institution’s customers to use a bank credit card at any card honoring merchant and to gain access to multiple ATM systems from a single ATM.

Interchange (fees) - Fees paid by one financial institution to another to cover handling costs and credit risk in a financial institution card transaction. Interchange fees generally flow toward the institution funding the transaction and assuming the risk. In a credit card transaction, the interchange fee is paid by the merchant acquirer accepting the merchant’s sales draft to the card-issuing institution, which, in turn, passes the fee to its merchants. In EFT/POS transactions, interchange flows in the opposite direction: the card-issuing institution (or customer) pays the fee to the terminal-owning institution. When a transaction is an off-line debit sale, the card-issuing institution collects an interchange fee from the merchant, rather than from the customer, unlike in an EFT/POS transaction, where the customer pays the interchange fee. Interchange revenue is derived from fees set by the card associations. Depending on the card association, fees can range from 1% to 3% of the value of the transaction. Interchange revenue is recognized as a card issuer’s second largest revenue line item.

Internet - A worldwide network of computer networks, governed by standards and protocols developed by the Internet Engineering Task Force (IETF).

Large value funds transfer system - A wholesale payment system used primarily by financial institutions in which large values of funds are transferred between parties.

Fedwire® and CHIPS are the two large-value transfer systems in the United States.

Lockbox - Deposit mechanism used by commercial firms and businesses to facilitate their deposit transaction volume. Typically, commercial firms and businesses direct customers to send payments directly to a financial institution address or post office box controlled by the institution. Financial institution personnel record payments received and prepare deposit slips, and subsequent processing proceeds as with other deposit taking activities.

Merchant acquirer - Bankcard association members that initiate and maintain contractual agreements with merchants for the purpose of accepting and processing bankcard transactions.

Merchant processing - Activity for the acceptance and settlement of bankcard products and transactions from merchants through the payment system.

Mobile financial services - A financial institution's use of mobile devices to provide products and services to its customers.

Multilateral netting settlement system - Multilateral netting is an arrangement among three or more parties to net their obligations. In these settlement systems transfers are irrevocable but are only final after the completion of end-of-day-settlement.

NACHA – The Electronic Payments Association (NACHA) - The national association that establishes the rules and procedures governing the exchange of ACH payments.

National Settlement Service (NSS) - Also referred to as Deferred Net Settlement. The Federal Reserve Banks' multilateral settlement service. NSS is offered to depository institutions that settle for participants in clearinghouses, financial exchanges, and other clearing and settlement groups. Settlement agents acting on behalf of those depository institutions electronically submit settlement files to the Federal Reserve Banks. Files are processed on receipt, and entries are automatically posted to the depository institutions' Reserve Bank accounts. Entries are final when posted.

Net debit cap - The maximum dollar amount of uncollateralized daylight overdrafts that an institution is authorized to incur in its Federal Reserve account. The net debit cap is generally equal to an institution's capital times the cap multiple for its cap category.

Office of Foreign Asset Control (OFAC) - The Office of Foreign Assets Control, United States Department of the Treasury, administers and enforces economic sanctions programs primarily against countries and groups of individuals such as terrorists and narcotics traffickers. The sanctions can be either comprehensive or selective, using the blocking of assets and trade restrictions to accomplish foreign policy and national security goals.

On-us checks - Checks that are deposited into the same institution on which they are drawn.

Originating depository financial institution (ODFI) - A participating financial institution that originates entries at the request of and by agreement with its originators in accordance with the provisions of the NACHA rules.

Paying bank - A paying bank is the institution where a check is payable and to which it is sent for payment.

Payment - A transfer of value.

Payment system - The mechanism, the rules, institutions, people, markets, and agreements that make the exchange of payments possible.

Payments System Risk Policy (PSR) - The Federal Reserve's Payments System Risk (PSR) policy addressing the risks that payment systems present to the Federal Reserve Banks, the banking system, and to other sectors of the economy.

Payroll card account - A bank account that is established directly or indirectly by an employer on behalf of an employee to which an electronic funds transfers the employee's wages or compensation on a recurring basis. The payroll card, often branded by one of the credit/debit card associations, provides the employee access to the funds.

Person-to-person (P2P) payment - Online payments using electronic mail messages to invoke a transfer of value between the parties over existing proprietary networks as on-us transactions.

Point-of-sale (POS) network - A network of institutions, debit cardholders, and merchants that permit consumers to make direct payment electronically at the place of purchase. The funds are withdrawn from the account of the cardholder.

Presentment fee - A fee that an institution receiving a check may impose on the institution that presents the check for payment. No presentment fee may be charged for checks presented by 8 a.m. local time.

Private label card - See "Store Card".

Real time gross settlement (RTGS) System - A type of payments system operating in real time rather than batch processing mode. It provides immediate finality of transactions. Gross settlement refers to the settlement of each transfer individually rather than netting. FedwireÒ is an example of a real time gross settlement system.

Receiver - An individual, corporation, or other entity that has authorized a company or an originator to initiate a credit or debit entry to a transaction account belonging to the receiver held at its RDFI.

Receiving depository financial institution (RDFI) - Any financial institution qualified to receive debits or credits through its ACH operator in accordance with the ACH rules.

Reconverting bank (Check 21) - The financial institution that creates a substitute check. With respect to a substitute check that was created by a person that is not a financial institution, the reconverting bank is the first financial institution that transfers, presents, or returns that substitute check or, in lieu thereof, the first paper or electronic representation of that substitute check. The reconverting bank warrants that (1) the substitute check is the legal equivalent of the original check; and (2) the original check cannot be presented again in any form so the customer pays the check only once.

Regulation CC - A regulation (12 CFR 229) promulgated by the Board of Governors of the Federal Reserve System regarding the availability of funds and the collection of checks. The regulation governs the availability of funds deposited in checking accounts and the collection and return of checks.

Regulation E - A regulation (12 CFR 205) promulgated by the Board of Governors of the Federal Reserve System to ensure consumers a minimum level of protection in disputes arising from electronic fund transfers.

Regulation Z - Regulation Z, the Truth in Lending Act (TILA) (12 CFR 226) promulgated by the Board of Governors of the Federal Reserve System. The regulation prescribes uniform methods for computing the cost of credit, disclosing credit terms, and resolving errors on certain types of credit accounts.

Remittance cards - Payment cards that are typically used to facilitate cross-border movement of funds by individuals and for person-to-person transactions.

Remote deposit capture (RDC) - A service that enables users at remote locations to scan digital images of checks and transmit the captured data to a financial institution or a merchant that is a customer of a financial institution.

Remotely created check (RCC) - A check that is drawn on a customer account at a financial institution, is created by the payee, and does not bear a signature in the format agreed to by the paying financial institution and customer. RCCs are also known as "demand drafts," "telechecks," "preauthorized drafts," "paper drafts," or "digital checks."

Reserve account - A non-interest-earning balance account institutions maintain with the Federal Reserve Bank or with a correspondent bank to satisfy the Federal Reserve's reserve requirements. Reserve account balances play a central role in the exchange of funds between depository institutions.

Reserve requirements - The percentage of deposits that a depository institution may not lend out or invest and must hold either as vault cash or on deposit at a Federal Reserve Bank. Reserve requirements affect the potential of the banking system to create transaction deposits.

Retail payments - Payments, typically small, made in the goods and services market.

Return (ACH) - Any ACH entry that has been returned to the ODFI by the RDFI or by the ACH operator because it cannot be processed. The reason for each return is included with the return in the form of a "return reason code." (See the NACHA "Operating Rules and Guidelines" for a complete reason code listing.)

Routing number - Also referred to as the ABA number. A nine-digit number (eight digits and a check digit) that identifies a specific financial institution.

Settlement - The final step in the transfer of ownership involving the physical exchange of securities or payment. In a banking transaction, settlement is the process of recording the debit and credit positions of the parties involved in a transfer of funds. In a financial instrument transaction, settlement includes both the transfer of securities by the seller and the payment by the buyer. Settlements can be "gross" or "net." Gross settlement means each transaction is settled individually. Net settlement means parties exchanging payments will offset mutual obligations to deliver identical items (e.g., dollars or EUROS), at a specified time, after which only one net amount of each item is exchanged.

Settlement date (ACH) - The date on which an exchange of funds with respect to an entry is reflected on the books of the Federal Reserve Bank.

Single-Entry (ACH) - A one-time transfer of funds initiated by an originator in accordance with the receiver's authorization for a single ACH credit or debit to the receiver's consumer account.

Standard Entry Class (SEC) code - Three-character code in an ACH company/batch

header record used to identify the payment type within an ACH batch.

Store card - A credit card issued by a financial institution for a specific merchant or vendor that does not carry a bankcard association logo. Store cards can only be used at the merchant or vendor whose name appears on the front of the card.

Stored-value card - A card-based payment system that assigns a value to the card. The card's value can be stored on the card itself (i.e., on the magnetic stripe or in a computer chip) or in a network database. As the card is used for transactions, the transaction amounts are subtracted from the card's balance. As the balance approaches zero, some cards can be "reloaded" through various methods and others are designed to be discarded. These cards are often used in closed systems for specific types of purchases.

Substitute check (Check 21) - Also known as the Image Replacement Document (IRD). A paper reproduction of an original check that (1) contains an image of the front and back of the original check; (2) bears a MICR line that, except as provided under ANS X9.100-140, contains all the information appearing on the MICR line of the original check when it was issued and any additional information that was encoded on the original check's MICR line before an image of the original check was captured; (3) conforms in paper stock, dimension, and otherwise with ANS X9.100-140; and (4) is suitable for automated processing in the same manner as the original check. The Federal Reserve Board of Governors can by rule or order determine different standards.

Third-party sender - A special subset of a technology service provider that is authorized to transmit ACH files on behalf of an originator. Typically, the ODFI must rely upon warranties by the third- party sender regarding the originators' identity and credit worthiness, which places additional risks on the ODFI.

Third-party service provider (TPSP)(For ACH) - A third party, other than the ODFI or RDFI, that performs any function on behalf of the ODFI or the RDFI related to ACH processing. These functions would include the creation and sending of ACH files or acting as a sending or receiving point on behalf of a participating depository financial institution.

Truncating bank (Check 21) - The financial institution that truncates the original check. If a person other than a financial institution truncates the original check, the truncating bank is the first financial institution that transfers, presents, or returns, in lieu of such original check, a substitute check or, by agreement with the recipient, information relating to the original check (including data taken from the MICR line of the original check or an electronic image of the original check), whether with or without the subsequent delivery of the original check.

USA Patriot Act - The USA PATRIOT Act (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (Public Law Pub.L. 107-56), commonly known as the "Patriot Act", was enacted by Congress to deter and punish terrorist acts in the United States and around the world by enhancing the law enforcement investigatory tools of both domestic law enforcement and foreign intelligence agencies.

WEB SEC code - An ACH debit entry initiated by an originator resulting from the receiver's authorization through the Internet to make a transfer of funds from a consumer account of the receiver.

Appendix C: Schematic of Retail Payments Access Channels & Payments Method

Retail payments can be categorized within two broad groups according to the access channel and the payment method. The access channel is used at the beginning of the transaction process and provides the user interface (e.g., a plastic card with a magnetic strip). The payment method includes the remaining parts of the payments process governed by applicable laws, regulations, and contracts.

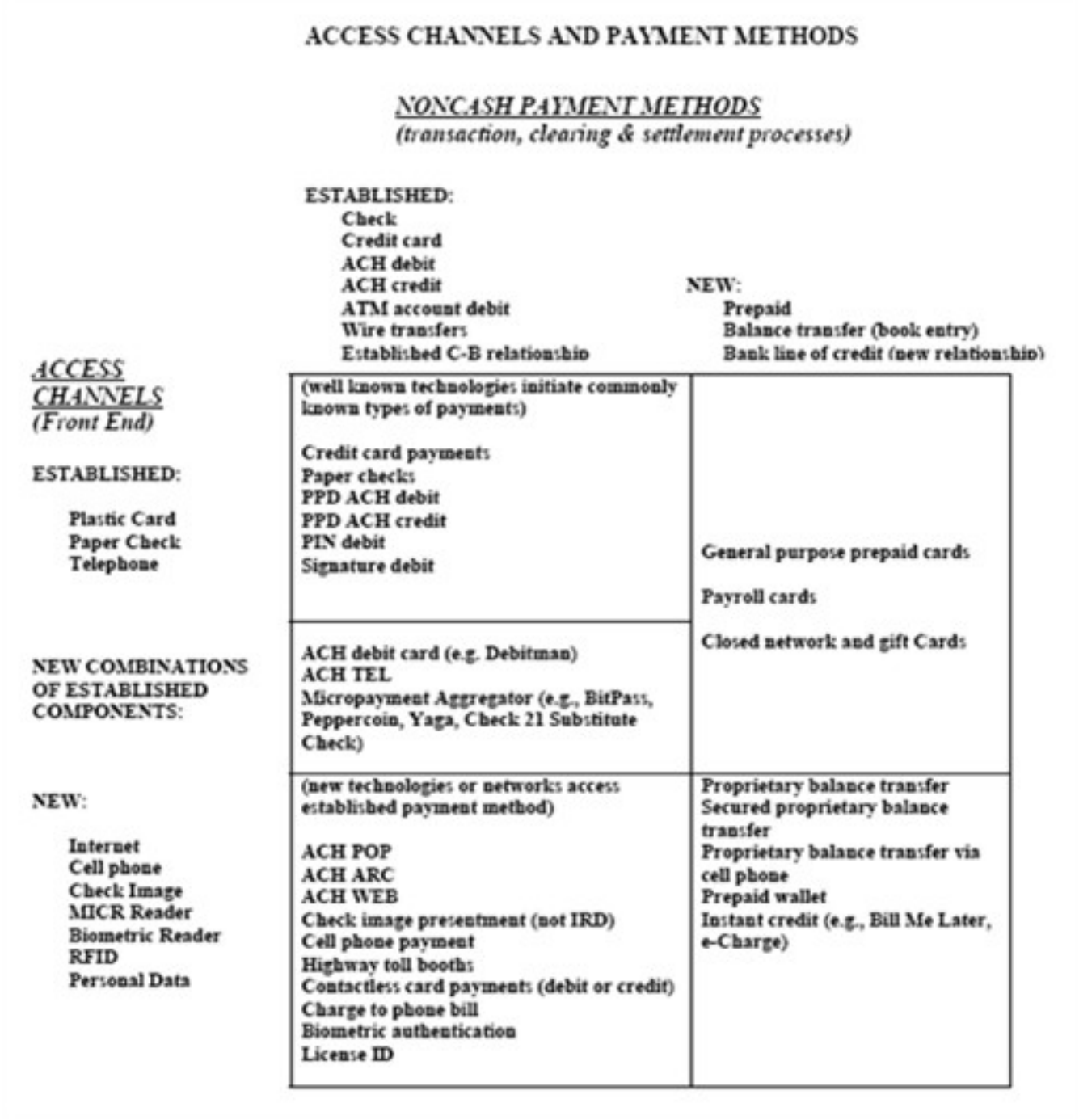


Figure 13

Payment methods that have the fewest changes from established methods are shown in the upper left quadrant above. The lower right quadrant includes emerging payment methods in terms of access channels and payment methods. The remaining two quadrants, upper right and lower left, are hybrids of new and established components. The left side of the matrix shows examples of access channels used to initiate payment

transactions, while the top of the matrix identifies general payment methods. The cells list a sample of the payment types that incorporate these various access and payment-method components. Retail payments may be effected using a variety of electronic networks in addition to the traditional cash and check processes. The electronic networks, which are discussed throughout this handbook, include the Automated Clearing House, card associations such as Visa, or MasterCard, and ATM networks.

Retail payment systems continue to evolve with advances in technology. These advances enable financial institutions to develop new products and services, to lower the barriers to business entry for smaller institutions, and to use "economies of scale."

Appendix D: Laws, Regulations, and Guidance

Laws

- 15 USC 1601: Truth in Lending Act (N/A)
- 12 USC 1861-1867(c): Bank Services Company Act (N/A)
- 12 USC 4001: Expedited Funds Availability Act (N/A)
- 12 USC 5001: Check Clearing for the 21st Century Act (N/A)
- 15 USC 1681m(e): Fair Credit Reporting Act (N/A)
- 15 USC 1693: Electronic Funds Transfer Act (N/A)
- 15 USC 6801 and 6805(b): Gramm-Leach-Bliley Act (N/A)
- 18 USC 1 (Pub. L. No. 107-56): USA Patriot Act (N/A)
- 31 USC 5311: Bank Secrecy Act (N/A)

Federal Financial Institutions Examination Council

- Authentication in an Internet Banking Environment (October 2005)
- Bank Secrecy Act/anti-Money Laundering InfoBase (N/A)
- Check 21 InfoBase (N/A)

Federal Reserve Board

- 12 CFR 210, Subparts A and B (Regulation J) (N/A)
- 12 CFR 205 (Regulation E) (N/A)
- 12 CFR 226, Truth in Lending (Regulation Z) (N/A)
- 12 CFR 229, Subparts A, B, and C (Regulation CC) (N/A)
- SR Letter 09-2: FFIEC Guidance Addressing Risk Management of Remote Deposit Capture Activities (January 14, 2009)
- Board of Governors of the Federal Reserve System Payments System Risk (PSR)

Policy (December 19, 2008)

- SR Letter 07-15: Release of Revised FFIEC Bank Secrecy Act/Anti-Money Laundering Examination Manual (August 24, 2007)
- SR Letter 05-19: Interagency Guidance on Authentication in an Internet Banking Environment (October 13, 2003)
- SR Letter 01-15: Safeguarding Customer Information (June 7, 2001)
- SR Letter 01-11: Identity Theft and Pretext Calling (April 26, 2001)
- SR Letter 00–17: FFIEC Guidance on the Risk Management of Outsourced Technology Services (November 30, 2000)
- SR Letter 00-04: Outsourcing of Information and Transaction Processing (February 29, 2000)
- SR Letter 93-64: Credit Card-related Merchant Activities (December 18, 1993)

Federal Deposit Insurance Corporation

- FIL 4-2009: Risk Management of Remote Deposit Capture (January 14, 2009)
- FIL 129-2008: New General Counsel's Opinion No. 8, Stored Value Cards and Other Nontraditional Access Mechanisms (November 13, 2008)
- FIL 127-2008: Guidance on Payment Processor Relationships (November 7, 2008)
- FIL 44-2008: Guidance on Managing Third-Party Risk (June 6, 2008)
- FIL 32-2007: Identity Theft - FDIC's Supervisory Policy on Identity Theft (April 11, 2007)
- Credit Card Activities Manual (March 2007)
- FFIEC Guidance Authentication in an Internet Banking Environment, FIL 103-2005 (October 2005)
- FIL 7-2005: Fair and Accurate Credit Transactions Act of 2003, Guidelines Requiring the Proper Disposal of Consumer Information (February 2, 2005)
- FIL 116-2004: Check Clearing for the 21st Century Act (October 27, 2004)
- FIL 39-2001: Identity Theft and Pretext Calling (May 9, 2001)
- FIL 79-98: Electronic Financial Services and Consumer Compliance (July 16, 1998)

National Credit Union Administration

- NCUA Letter to Credit Unions, 09-CU-01: Risk Management of Remote Deposit Capture (with Enclosure) (January 2009)
- NCUA Letter to Credit Unions, 07-CU-13: Supervisory Letter - Evauluation Third Party Relationships (December 2007)
- NCUA Corporate Credit Union Guidance Letter 07-04: Accounting for Future-Dated Automated Clearing House (ACH) Transactions (October 2007)
- NCUA Letter to Credit Unions 06-CU-14: Bank Secrecy ACT (BSA)/Anti-Money Laundering (AML) Manual Interagency Outreach (September 2006)
- NCUA Letter to Credit Unions 05-CU-18: Guidance on Authentication in Internet Banking Environment (November 2005)
- NCUA Letter to Credit Unions 05-CU-16: Bank Secrecy Act Compliance (October 2005)
- NCUA Regulatory Alert 05-RA-02: Suspicious Activity Reports on OFAC blocked transactions (January 2005)
- NCUA Regulatory Alert 04-RA-12: Check 21 Act (October 2004)
- NCUA Regulatory Alert 03-RA-07: Final Patriot Act Regulations on Customer (Member) Identification (May 2003)
- 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)
- NCUA Regulatory Alert 01-RA-08: Interim Final Rules Amending Regulations B, E, M, Z, and DD - Electronic Delivery of Required Disclosures (August 2001)
- NCUA Letter to Credit Unions, 00-CU-11: Risk Management of Outsourced Technology Services (with Enclosure) (December 2000)
- NCUA Regulatory Alert 99-RA-3: Pretext Phone Calling by Account Informa-tion Brokers (February 1999)

Office of the Comptroller of the Currency

- Office of the Comptroller of the Currency (OCC) Comptroller's Handbook: Depository Services (November 19, 2008)
- OCC Bulletin 2009-4: Remote Deposit Capture: Interagency Guidance (January 14, 2009)
- OCC Comptroller's Handbook: Truth in Lending (October 6, 2008)
- OCC Bulletin 2008-12: Payment Processors: Risk Management Guidance (April 24,

2008)

- OCC Bulletin 2006-39: Automated Clearing House Activities: Risk Management Guidance (September 1, 2006)
- OCC Bulletin 2006-06: Bank Secrecy Act/Anti-Money Laundering: Joint Statement on Sharing Suspicious Activity Reports with Controlling Companies (January 27, 2006)
- OCC Bulletin 2005-13: Response Programs for Unauthorized Access to Customer Information and Customer Notice: Final Guidance (April 14, 2005)
- OCC Advisory Letter 2004-6: Payroll Card Systems (May 14, 2004)
- OCC Bulletin 2003–01: Credit Card Lending, Account Management and Loss Allowance Guidance (January 8, 2003)
- OCC Comptroller's Handbook: Merchant Processing (December 2001)
- OCC Bulletin 2001-47: Third Party Relationships, Risk Management Principles (November 1, 2001)
- OCC Bulletin 2001-6: Expanded Guidance for Subprime Lending Programs (January 31, 2001)
- OCC Advisory Letter 2000-10: Payday Lending (November 27, 2000)
- OCC Advisory Letter 2000-9: Third-Party Risk (August 29, 2000)
- OCC Advisory Letter 2000-6: Audit and Internal Controls (July 23, 2000)
- OCC Bulletin 2000-20: FFIEC Uniform Retail Credit Classification and Account Management Policy (June 22, 2000)
- OCC Bulletin 2000-16: Risk Modeling, Model Validation (May 30, 2000)
- OCC Bulletin 2000-3: FFIEC Consumer Credit Reporting Practices (February 16, 2000)
- OCC Bulletin 99-15: Subprime Lending: Risks and Rewards (April 5, 1999)
- OCC Bulletin 99-10: Interagency Guidance on Subprime Lending (March 5, 1999)
- OCC Bulletin 98-3: Technology Risk Management: Guide for Bankers and Examiners (February 4, 1998)
- OCC Bulletin 97-24: Credit Scoring Models, Examiner Guidance (May 20, 1997)
- OCC Advisory Letter 96-7: Credit Card Pre-Approved Solicitations (September 26, 1996)

Office of Thrift Supervision

- 12 CFR Part 570: Interagency Guidelines Establishing Standards for Safeguarding Customer Information, Appendix B (N/A)
- RB 37-37: Electronic Fund Transfer Act (May 5, 2009)
- CEO Letter 291: Risk Management of Remote Deposit Capture (January 14, 2009)
- CEO Letter 273: Compliance with Truth in Savings and Electronic Transfer Act Rules: Government Accountability Office Report 08-281 (April 25, 2008)
- CEO Letter 228: Interagency Guidance on Authentication in an Internet Banking Environment (October 13, 2005)
- CEO Letter 214: Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice (March 30, 2005)
- RB 37-10: Check 21 (February 18, 2008)
- Thrift Bulletin 82a: Third Party Arrangements (September 1, 2004)
- CEO Letter 90: FFIEC Information Technology Examination Handbook- Audit Booklet, Electronic Banking Booklet (July 23, 1998)
- CEO Letter 113: Internal Controls (July 14, 1999)
- Examination Handbook: Section 218, Credit Card Lending (N/A)
- Thrift Activities Handbook: Section 340, Internal Control (December 2003)
- Thrift Activities Handbook: Section 341, Technology Risk Controls (January 2002)
- Thrift Activities Handbook: Section 580, Payment Systems Risk (January 1994)
- Examination Handbook: Section 1330, Electronic Funds Transfer Act (N/A)
- Examination Handbook: Section 1335, Expedited Funds Availability Act (N/A)
- Examination Handbook: Section 1336, Check 21 (N/A)
- Check Clearing for the 21st Century Compliance InfoBase, OTS Press Release 04-43 (October 2004)

Appendix E: Mobile Financial Services

AppE.1 Introduction

Mobile financial services (MFS) are the products and services that a financial institution provides to its customers through mobile devices. [54] The mobile channel [55] provides an opportunity for financial institutions of all sizes to increase customer access to financial services and decrease costs. Although the risks from traditional delivery channels for financial services continue to apply to MFS, the risk management strategies may differ. As with other technology-related risks, management should identify, measure, mitigate, and monitor the risks involved and be familiar with technologies that enable MFS.

AppE.1.a Purpose and Scope

This appendix focuses on risks associated with MFS and emphasizes an enterprise-wide risk management approach to the effective management and mitigation of those risks. This appendix also discusses the technologies used in the mobile channel and may be helpful to the board and management for the integration of MFS into the institution's risk management program. The risks and controls addressed in this appendix, however, are not exhaustive. Additionally, this appendix contains a set of work program objectives to help the examiner determine the inherent risk and adequacy of controls at an institution or third party providing MFS.

AppE.1.b Background

MFS involve the use of a mobile device to conduct banking transactions and to initiate retail payments. Customers' mobile transactions often emulate those initiated on traditional desktop computers; however, MFS can provide more convenient transaction execution capabilities, such as the initiation or acceptance of mobile payments. MFS can pose elevated risks related to device security, authentication, data security, application security, data transmission security, compliance, and third-party management. Customers are often less likely to activate security controls, virus protection, or personal firewall functionality on their mobile devices, and MFS often involve the use of third-party service providers. This appendix addresses the following:

- MFS technologies.
- Risk identification.
- Risk measurement.

- Risk mitigation.
- Monitoring and reporting.

AppE.2 Mobile Financial Services Technologies

Financial institutions implement and offer MFS through technologies such as the following:

- Short message service (SMS)/text messaging.
- Mobile-enabled Web sites and browsers.
- Mobile applications.
- Wireless payment technologies.

AppE.2.a Short Message Service

SMS is a text messaging service component of phone, Web, or mobile communication systems. SMS uses standardized communications protocols to allow devices to exchange short text messages. Messages are typically limited to 160 characters and communicate either between mobile devices or between businesses and mobile devices (e.g., financial institutions requesting customer verification of transactions). Within the context of MFS, a customer uses SMS to provide financial transaction instructions to their financial institution. Financial institutions use SMS to provide information to customers, including account alerts or to communicate one-time passwords for Web site authentication.

AppE.2.b Mobile-Enabled Web Sites

A mobile device's browser allows customers to access a financial institution's Web site. Many financial institutions provide mobile-enabled Web sites, in addition to their regular Web site, which may improve the customer experience. The mobile-enabled Web site is designed to detect the type of device the customer is using (e.g., mobile device or desktop computer) and displays Web pages in the best format for that device.

AppE.2.c Mobile Applications

Mobile applications are downloadable software applications developed specifically for use on mobile devices. Mobile financial applications are developed by or for financial institutions to allow customers to perform account inquiries, retrieve information, or initiate financial transactions. This technology leverages features and functions unique to each type of mobile device and often provides a more user-friendly interface than is possible or available with either SMS or Web-based mobile banking.

AppE.2.d Wireless Payment Technologies

Customers may use mobile technologies to initiate wireless payments at point-of-sale (POS) terminals, make person-to-person (P2P) payments, or make other types of wireless payments, such as parking meter and mass transit access payments. Mobile wallets [56] allow customers to make wireless payments with a virtual payment card, as opposed to a physical card. The exchange of payment credentials and authorization between the mobile device and the payment recipient can use different core technologies. Technologies that provide the ability to make wireless payments include the following:

- **Near field communication (NFC)**: Wireless protocol that allows for exchange of payment credentials stored on the mobile device and other data at close range. For example, NFC is used to facilitate mobile payment systems developed by mobile phone manufacturers in conjunction with issuing financial institutions.
- **Image-based**: Coded images similar to bar codes used to initiate payments. Credentials may be encoded within an image or stored in the cloud. For example, specific retailers use quick response (QR) codes [57] to identify customers in a closed-loop mobile payment [58] system.
- **Carrier-based**: Payments billed directly to a customer's mobile carrier account. Merchants are paid directly by the mobile carrier, bypassing traditional payment networks. For example, a carrier-based payment may occur when mobile users donate money to charity through SMS messages.
- **Mobile P2P**: Payments initiated on a mobile device using the recipient's mobile phone number, e-mail address, or other identifier. Payment is through established retail payment technologies. For example, customers may download a P2P mobile application from their financial institution that allows them to send money to other users enrolled in the institution's system.

Although these technologies help facilitate financial institution-centric mobile payments, established retail payments channels (automated clearing house (ACH), credit/debit networks, electronic funds transfer (EFT), and intra-account transfers) remain the principal methods by which mobile payments are funded [59] and settled in the U.S. marketplace. With traditional retail payments channels serving as the backbone of mobile payments, users typically are required to provide verifiable financial institution account information or a credit, debit, or prepaid card to establish and fund a mobile payments service. The traditional retail payments channels allow financial institution

mobile payments providers to leverage existing banking relationships to verify identities, satisfy federal anti-money laundering requirements, and fund accounts.

AppE.3 Risk Identification

Management should identify the risks associated with the types of MFS being offered as part of the institution's strategic plan. Management should incorporate the identification of risks associated with mobile devices, products, services, and technologies into the financial institution's existing risk management process. The complexity and depth of the MFS risk identification varies depending on the functionality provided through the mobile channel and the type of data in transit and at rest.

The identification process should include risks at the institution and those associated with the use of mobile devices where the customer implements and manages the security settings. In providing customers with avenues for performing banking activities through mobile devices, an institution may transfer to the customer the ability to implement security settings. This transfer increases dependence on the customer to manage the controls over sensitive financial data. Additionally, there are numerous types of mobile devices that present different risks, and management should identify unique risks associated with specific devices. Before implementing mobile products and services, management should identify the associated risks, particularly in the areas of strategic, operational, compliance, and reputation risks.

AppE.3.a Strategic Risk

When financial institution management fails to incorporate its decisions regarding MFS into its strategic planning, the institution's level of strategic risk may increase. Management should identify the risks associated with the decision to offer MFS and determine what types of MFS best fit with the strategic vision, goals, and risk appetite of the institution.

AppE.3.b Operational Risk

MFS introduce unique operational risks. Management should identify the risks involved with transaction initiation, authentication and authorization, and the MFS technology itself. Some of the operational risks are associated with the mobile device and how the device communicates with the POS or other similar terminal. [60] Additionally, the varying access points [61] provide challenges with authentication and security.

MFS provide the opportunity to leverage tools and techniques not available in traditional banking payment products. The prevalence of mobile devices, common operating systems, and downloadable applications make these devices a target for malware and viruses. Without implementing additional controls, basic device access controls such as personal identification numbers (PIN) may not be adequate to protect data that is stored

on a mobile device because these controls could be circumvented by someone who has unrestricted physical access to the device. Additionally, a fraudster can compromise mobile application-based financial services by developing rogue, corrupted, or malicious applications (or adding rogue code to applications) that a customer downloads to his or her mobile device. Therefore, management should consider the implications of operational risks when evaluating and implementing such technologies.

AppE.3.b(i) SMS Technology Risk

SMS technology presents a number of security-related risks. SMS messages typically are transmitted unencrypted over widely used telecommunications networks. The messages are also vulnerable to spoofing, [62] which allows an unauthorized user to send an SMS message pretending to be from a different mobile number to mislead a customer into providing sensitive information to the unauthorized user. Similarly, fraudulent SMS messages may mislead customers into revealing financial institution account information or information used to access financial institution systems.

AppE.3.b(ii) Mobile-Enabled Web Site Risk

Mobile-enabled Web sites rely on existing Internet security protocols, which make the sites subject to many of the same vulnerabilities [63] that can compromise computer-based banking. Additionally, mobile devices can be limited by their hardware and operating systems, which can result in a reduced level of security. Mobile Web browsers are common starting points for malicious attacks, and malicious messages can come from many other sources. [64] Whereas desktop browsers have anti-phishing [65] and anti-cross-site scripting (anti-XSS) capabilities [66] to filter out the malicious code from Web sites, mobile-enabled browsers do not always have such features. The lack of anti-phishing and anti-XSS modules can increase the possibility of loss of sensitive information when using a mobile device.

As is the case with any Web-based application, attacks involving unvalidated "redirects and forwards" [67] can be used to maliciously craft a URL [68] to bypass the application's access control check and then provide the attacker access to privileged functions that normally would not be accessible to them. The attacks also can lead to malware download and installation. By modifying a URL and redirecting the browser to a malicious site, an attacker may successfully launch a phishing scam and steal user credentials.

Users often find it difficult to recognize a phishing message or a forged Web site, or determine whether a site is safe. Additionally, mobile browsers displayed on small screens may not effectively display the same visual security cues more easily seen on full-scale browsers on large screens.

AppE.3.b(iii) Mobile Application Risk

Applications can be downloaded onto mobile devices from a number of application stores. Although device manufacturer-authorized application stores perform due diligence, applications may still contain vulnerabilities that cause risks to the user and the financial institution. On some mobile devices, it is possible to download an application from application stores not authorized by the manufacturer, which poses a greater risk of users being exposed to malicious code because the applications may not be adequately reviewed by the store. Distribution of malware through applications is a material risk to the institution and its customers because of malware's ability to compromise sensitive data and monitor communications.

Another risk to the institution and its customers occurs with the end user's ability to access root user [69] privileges in the operating system of the device. The process to gain access is known as "rooting." Another method of removing the manufacturer's device controls or core operating system controls is "jailbreaking." Jailbreaking provides the user with additional access to and control over the device's operating and file systems, including the ability to circumvent security controls. For certain mobile devices, rooting and jailbreaking allow the user to download applications from untrusted sources, which may introduce malware onto the device.

Many applications store usernames, passwords, and e-mail addresses in clear text. Because users often have the same usernames and passwords across systems, it is possible to use the information obtained from a poorly designed mobile application to compromise user accounts on other systems. Mobile applications collect personal information (e.g., name, account number, and other personal details) and track user activity (e.g., purchases and location). These data are valuable to attackers and can result in compromised user privacy. Without properly securing the mobile application, unauthorized users can gain access to the back-end databases containing confidential information.

The mobile ecosystem is the collection of carriers, networks, platforms, operating systems, developers, and application stores that enable mobile devices to function and interact with other devices. Vulnerabilities may exist in any area of this decentralized mobile ecosystem and, therefore, result in a multi-entity patch management process among mobile device operating system developers, device manufacturers, wireless carriers, and other application developers. As a result of the decentralized ecosystem of some devices, a known vulnerability may remain unremediated while the various parties review, update, and ensure compatibility with their applications and the security mitigation. Additionally, integrating MFS application functionality with other applications and services on the customer's device may introduce vulnerabilities because MFS applications are not built in or native to the device.

AppE.3.b(iv) Mobile Payments Risk

The portability of mobile devices can lead to the devices being misplaced or stolen, which may allow unauthorized access to the mobile wallet or user credentials. Such access can result in unauthorized payments and funds transfers and fraudulent purchases.

Because mobile payments at the POS may use NFC, communications between the device and the POS terminal can be intercepted, while the device is in the user's possession. Even if these communications are encrypted, which they are not by default, there remains a potential for unauthorized access to transaction information, which could be used to perpetrate financial fraud.

Vulnerabilities create the potential to take advantage of weak security controls in the payment provisioning or enrollment functions of the NFC payment system process to commit fraud. Malicious actors using stolen identity information (e.g., from credit reports, tax records, health care records, and employee records) may establish fake accounts on NFC-enabled mobile devices to make unauthorized transactions. [70]

AppE.3.c Compliance Risk

Financial institution management should identify the compliance risks as it determines which MFS to offer and continue to monitor these risks as the technology for MFS evolves. Consumer laws, regulations, and supervisory guidance that apply to a given financial product or payment method generally apply regardless of the technology used to provide the products and services.

One of the challenges in providing MFS is that a significant portion of the innovation in the industry is driven by entities outside of the traditional financial services sector. These entities may be unfamiliar with regulatory requirements and supervisory expectations that apply to regulated financial institutions and their service providers. Management should understand how the institution's risk profile changes when it uses any third party, but particularly a third-party service provider that is unfamiliar with the regulation and supervision of the financial services sector, to design applications.

AppE.3.d Reputation Risk

Management should identify and consider how providing MFS may create reputation risk. Reputation risk is particularly relevant in the context of privacy and data security, as public scrutiny of the treatment of customer information continues to grow. The mobile channel, with many of its activities trending toward personalization [71] and transmission of data, poses a risk of disclosure of personal information. Additionally, services provided by a third party that are not implemented appropriately or securely may expose the financial institution to reputation risk if interruptions in service occur or sensitive customer information is compromised.

AppE.4 Risk Measurement

The identification of risks should be followed by a measurement of the level and types of risks involved in offering MFS. Management should measure potential risks across all applicable risk categories. This assessment may help management determine the likelihood and impact of the risks affecting the institution. The results should be prioritized to determine which controls may be appropriate for the services provided by the institution. This process should be ongoing and updated whenever management implements a change to the strategy or MFS.

AppE.5 Risk Mitigation

Effective enterprise-wide risk management helps management determine whether controls are effective and goals are compatible with the financial institution's risk appetite and strategic plan. When offering MFS, management should mitigate identified risks by implementing effective controls across the institution. As is the case with any new product offering, management should develop and implement policies and procedures to

comply with applicable laws and regulations and require appropriate internal controls for security and confidentiality of the MFS transactions. As part of the institution's audit of retail payments systems, audit coverage should include MFS.

Unlike many financial services that allow institutions to control much of the interaction, MFS typically require the coordinated and secure exchange of information among several unrelated entities. Depending on the type of MFS offered, institutions may find that the effective management of risks involves interaction with application developers, mobile network operators, device manufacturers, specialized security firms, and other nonfinancial third-party service providers. Additionally, financial institution management should provide security awareness materials to the institution's customers, which may include prudent security practices for the device (e.g., use of mobile anti-malware, PIN protection) so that customers understand their roles in securing the device and the need for such security.

AppE.5.a Strategic Risk Mitigation

Financial institution management should incorporate decisions on providing MFS into its strategic planning process. Various elements should be part of any mobile strategy, including the products and services to be offered, types of transactions allowed, limits over transaction amounts, mobile architecture design, supported mobile devices, customer needs, and use of third parties.

AppE.5.b Operational Risk Mitigation

Financial institution management should develop a layered approach to mitigate operational risks from MFS. This may include implementing security techniques at the server and database level; using transaction monitoring and geolocation techniques to identify anomalous MFS transactions; implementing and refining fraud prevention, detection, and response programs that facilitate rapid notification of potentially fraudulent transactions; applying additional controls (e.g., stronger authentication, encryption) to prevent unauthorized access to sensitive customer information stored on the device; and educating customers and employees to identify social engineering attempts that could lead to fraud.

The following are general operational controls that an institution should consider when implementing MFS.

- **Enrollment.** Financial institution management should have appropriate controls and communication of policy and procedures to verify a customer's identity when enrolling customers in mobile payment systems used at the point of sale (e.g., allowing a customer with a physical payment card the ability to enroll that card into the customer's mobile wallet).
- **Authentication and authorization.** A financial institution should have a process for authenticating users of MFS to protect customers against fraudulent transactions or

malicious activities. Depending on the technology used and associated level of risk, financial institutions may consider biometric (e.g., voice, fingerprint, facial recognition) or out-of-band [72] authentication processes. The financial institution should not use mobile payment applications that rely on less secure (e.g., single factor) methods of authentication. [73]

- **Application development and distribution.** The application development life cycle should include a thorough design and architecture review using threat-modeling [74] techniques to reduce potential risks and meet the financial institution's security objectives. Additionally, application developers should develop applications using secure coding techniques, [75] and applications should be rigorously tested for vulnerabilities (e.g., detailed code analysis and white-hat hacking [76]) at least annually. Institutions should distribute applications and updates securely and in a timely fashion. Management should consider designing anti-malware capabilities into mobile applications. Applications should not retain sensitive customer information on the device, such as user IDs and passwords, and the application should securely wipe any sensitive customer information from memory when the customer exits the application. If a third party developed the application, the third-party developer should incorporate these control requirements into its development process.

- **Application security.** Management should ensure that the institution's MFS contain log-on credentials in addition to those used to access the device. Management should employ multi-factor authentication or layered security controls depending on the types and volumes of transactions. The system should require re-authentication whenever the device or MFS is unused for a designated period and each time the user launches the application.

- **Contracts.** The institution should use well-constructed contracts, developed with legal counsel, to mitigate its risks from third parties. Contracts should be appropriate for the institution's specific mobile strategy and should clearly identify each party's roles and responsibilities. Financial institution management may need to establish contracts with the institution's customers and third parties that cover types of data collected and circumstances related to data sharing.

- **Customer awareness.** Financial institution management should make reasonable efforts to educate customers about the need to maintain the physical and logical security [77] of mobile devices and suggest that users regularly install operating system and firmware updates. Management should make clear that customers should download applications only from reputable sources, and the institution's Web site should have a link to the source of any institution-approved applications. Institutions should have customer security awareness materials available to help customers understand the risks involved in using MFS, including the use of unsecured "public" wireless networks. Financial institutions should suggest that customers consider running anti-malware software on their mobile devices, if possible.

- **Logging and monitoring.** Management should have logging and monitoring capabilities on all MFS to track customer activity and security changes and identify anomalous behavior and transactions.

AppE.5.b(i) SMS Technology Risk Mitigation

Financial institution management should employ compensating controls (e.g., redacting

customer account numbers when sent via SMS) to mitigate the inability to encrypt SMS messages. Additionally, management should limit the access or functionality available to the customer through SMS banking. When the transaction risk is more significant, management should consider other risk mitigation methods, including pre-registration and the use of security tokens. PINs also could be employed, but are often easier to break and harder to remember. To strengthen the security of PIN usage, management can implement specific requirements (e.g., requiring them to be regularly changed). An institution should update its customer awareness materials to include information on avoiding phishing messages by SMS.

AppE.5.b(ii) Mobile-Enabled Web Site Risk Mitigation

Financial institution management should consider several controls to mitigate risks associated with mobile-enabled Web sites, including the following:

- Provide specific training and security awareness materials for users and customers accessing the institution's sites to teach them how to identify compromised sites.
- Require Web site developers to follow a secure development life cycle to increase the security of the Web sites designed for the financial institution.
- Require developers to build a secure Web site especially for mobile devices and encourage them to follow the guidelines provided from the Open Web Application Security Project (OWASP) [78] Top 10 for Web application and OWASP Top 10 for mobile.
- Make available a baseline set of controls, and educate customers on the use of those controls to protect their device and information (e.g., device passwords with complexity, application passwords, and an auto-wipe feature after excessive password failures).
- Determine whether mobile browsers have available safeguards implemented, such as anti-XSS modules or additional monitoring of browsers for those that are no longer supported, and deny access to devices with mobile browsers not meeting minimum standards.
- Determine whether mobile-enabled Web sites are designed with the following mitigating controls to help minimize the potential for exploitation of "redirect and forward" vulnerabilities:

- Avoid using redirects and forwards.

- Explicitly hard code the URL to prevent manipulation by an attacker.

- Apply additional validation or control checks to verify the user trying to access the URL, validate the URL, check the appropriateness of the URL request, and prevent a malicious user from redirecting site users to a phishing, malicious, or nonaffiliated site.

- Create a whitelist [79] of trusted URLs.

- Force all redirects to go through a page that notifies a user that he or she is leaving the page and require user confirmation.

- Perform frequent vulnerability scans.

AppE.5.b(iii) Mobile Application Risk Mitigation

Management should consider the use of a variety of security mechanisms for mobile applications and should evaluate, prioritize, and implement appropriate mitigating controls, including the following:

- Employing tools, such as policy enforcement and device fingerprinting, to determine whether a customer's mobile device will be allowed to access the institution's MFS by validating device characteristics (e.g., level of security controls, operating system type, operating system version, whether the mobile device is rooted or jailbroken, and patch status).
- Providing security awareness training to end users to help them recognize legitimate applications and provide a list of reputable sites to download institution-approved applications.
- Performing security testing at all post-design phases of the system development life cycle for all applications. Establishing a process to deactivate older application versions that no longer meet minimum security requirements or prompt the end user to upgrade to an acceptable version.
- Providing basic customer education relative to security to mitigate the risks associated with rooted or jailbroken devices.
- Designing applications to ensure that critical information, such as passwords and credit card numbers, does not reside directly on a device. If critical information resides directly on a device, it should be stored securely (e.g., within an encrypted data section or within encrypted storage in the file system).
- Establishing processes when implementing mobile applications to collect only necessary information and appropriately secure that information and any related analytics reporting available within or external to the mobile application.
- Designing applications to mitigate the risk of unpatched devices or those that are no longer supported by the manufacturer.
- Securing back-end servers containing the MFS application and customer data to prevent unauthorized users from accessing data. If a third party manages the application and back-end server, validate that the third party implements appropriate security measures.
- Developing applications in a "sandbox," [80] which creates a more secure area within the device from which to process transactions.
- Maintaining awareness of vulnerabilities through online forums, vendor sites, and U.S. Computer Emergency Readiness Team (US-CERT) or Financial Services-Information Sharing and Analysis Center (FS-ISAC) alerts. The vulnerabilities may affect unpatched and unsupported operating system versions. Take a risk-based approach when offering MFS to customers using unpatched and unsupported operating system versions and recommend to customers that they upgrade to more secure software, operating systems, and devices when appropriate.

- Periodically testing the functionality of MFS applications with other integrated mobile applications and services.

AppE.5.b(iv) Mobile Payments Risk Mitigation

Mitigating controls in mobile payments should include discussions between the financial institution and its mobile payments provider to identify and minimize potential risk factors. Financial institution management should work with mobile-payments platform developers to encourage the use of the following:

- Traffic filtering to help prevent or minimize denial-of-service attacks. [81]
- Trusted platform modules. [82]
- Secure telecommunications protocols (e.g., secure sockets layer/transport layer security [SSL/TLS]).
- Tokenization In the context of data security, [83] to limit the transmission of account information.
- Encryption to minimize the opportunity for the interception of traffic.
- Anti-malware software.
- Authentication controls of both the user and application.
- Encryption of personal information stored on the mobile device.

AppE.5.c Compliance Risk Mitigation

Institution management and system designers should consult with compliance staff to minimize compliance risks when developing and implementing MFS. Financial institution management should reassess its current mobile service offerings regularly and, in conjunction with appropriate compliance and legal staff, examine applicable laws and regulations, including those for consumer protection, to determine which may apply to their specific mobile financial service offerings. The compliance officer should take the following steps:

- Determine whether applicable disclosure requirements are fully accessible on the mobile device.
- Review the institution's existing compliance management system and ability to make appropriate modifications to policies and procedures to address the products, services, and operating features of the MFS technology.
- Monitor for any legal and regulatory changes that may be applicable to MFS on an

ongoing basis.

- Train institution staff regarding compliance implications of MFS.

AppE.5.d Reputation Risk Mitigation

To protect its brand reputation, management should adopt appropriate and effective controls over customer information accessed, transmitted, or stored by the MFS to minimize or prevent disclosure of personal information and the potential for fraudulent transactions. Management should implement such controls whether it is providing the MFS directly or through a third party.

AppE.6 Monitoring and Reporting

Financial institution management should have appropriate performance monitoring systems for assessing whether the product or service is meeting operational expectations. Such systems should do the following:

- Include limits on the level of acceptable risk exposure that management and the board are willing to assume.
- Identify specific objectives and performance criteria, including quantitative benchmarks for evaluating success of the product or service.
- Periodically compare actual results with projections and qualitative benchmarks to detect and address adverse trends or concerns in a timely manner.
- Modify the business plan, when appropriate, based on the performance of the product or service. Such changes may include exiting the activity should actual results fail to achieve projections.

A variety of reports can facilitate management oversight of MFS activities. Management should structure the report content to meet the needs of the various levels of management. Reports should address point-in-time as well as trend activity for both individual customers and mobile channel activities to compare actual trends with the mobile strategy. Reports for new services should emphasize the volume of activity from the onset and report on changes in usage or volume over time. Management should develop reports to document the various demographic and industry sectors served and monitor changes in these areas to determine whether the MFS offered are meeting the institution's strategy or should be refined.

AppE.7 Mobile Financial Services Work Program

Objective 1: Management effectively responds to issues raised or problems related to MFS.

1. Review examination documents and financial institution reports for outstanding issues or problems related to MFS. Consider the following:

a. Pre-examination planning memos.

b. Prior regulatory reports of examination.

c. Prior examination work papers.

d. Internal and external audit reports, including SSAE 16 [84] reports.

2. Financial institution's overall risk assessment and strategic plan.

3. Review management's response to audit recommendations on MFS, if any, noted since the prior examination. Consider the following:

1. a. Adequacy and timing of corrective action.
2. b. Resolution of root causes rather than just specific audit deficiencies.
3. c. Existence of any outstanding issues.
4. d. Monitoring systems used to track the implementation of recommendations on an ongoing basis.

Objective 2: Financial institution management incorporates (or plans to incorporate) its plan for implementing MFS into its strategic planning process.

1. Determine whether financial institution management has an MFS strategy to identify the types of MFS that management plans to offer.
2. Describe the MFS that the financial institution offers. Determine whether the institution offers or implements MFS through one or more of the following technologies:

1. a. SMS.
2. b. Mobile-enabled Web sites or browsers.
3. c. Mobile applications.
4. d. Technologies that enable mobile payments.

Objective 3: Financial institution management identifies the risks associated with offering

MFS.

1. After the MFS strategy is complete, determine whether the institution developed an effective risk assessment process for the MFS offerings. Verify whether management incorporates the results of the risk assessment into a process to periodically review and update the strategy.
2. Review whether the risk identification process includes risks associated with MFS, particularly in the areas of strategic, operational, regulatory, and reputation risks.
3. With respect to strategic risk, determine whether management identified the risks associated with the decision to offer MFS and whether that is consistent with the strategic vision, goals, and risk appetite of the institution.
4. Determine whether management considered and identified operational risks associated with MFS, including risks involved with the following:

1. a. Transaction initiation and completion.
2. b. Authentication and authorization.
3. c. Technology used for MFS.
4. d. Mobile devices.
5. e. Method of communication between the device and the terminal accepting payment.
6. f. Authentication and security of access points.
7. g. Fraud tools and techniques.
8. h. Current and emerging threats to mobile applications, weaknesses in mobile application security, and prevalence of mobile devices, common operating systems, and downloadable applications.
9. 5. Determine whether management also considered the implications of operational risks specific to technologies used to implement MFS. Specifically, review whether management appropriately identified the differing risks related to the following technologies:

1. a. SMS: Include the lack of security through unencrypted text messages; SMS spoofing; and fraudulent text messages (phishing).
2. b. Mobile-enabled Web sites: Include vulnerabilities with Internet banking (hardware, operating system, and security limitations); malicious messages through Web-based attack vectors; limitations on anti-phishing and anti-XSS capabilities; malicious attacks through unvalidated redirects and forwards; user constraints on recognizing phished or forged sites; and limitations on visual security cues.

3. **c. Mobile application**: Include application vulnerabilities (e.g., unpatched and outdated applications); malware; ability to jailbreak or root devices; use of unapproved application stores; weak storage controls over confidential information on devices; and inappropriate access to back-end databases.

4. **d. Mobile payments**: Include loss or theft of mobile devices leading to unauthorized payments, funds transfers, and credit card purchases; interception of NFC communications; and weak security controls in the payment provisioning process.

1. 6. With respect to compliance risk, determine whether management identified the applicable risks related to MFS. Review whether management understands that the consumer laws, regulations, and supervisory guidance that apply to a given financial product or payment method generally apply regardless of the technology used. Additionally, determine whether management identified risks associated with the use of nontraditional third-party service providers often found in the innovation and development sphere of MFS.

1. 7. With respect to reputation risk, determine whether management identified the following:

1. a. Potential reputation risk that may arise from providing MFS, including issues related to privacy and data security.

2. b. Risks associated with the decision to outsource the development and maintenance of mobile products and the effect of third parties on the institution's risk profile.

Objective 4: Financial institution management appropriately and effectively measures risks associated with MFS and determines the likelihood and impact of those risks.

1. Determine whether management effectively measures risks and determines the likelihood and impact of those risks.

2. Determine whether management effectively prioritizes measured risks.

3. Determine the effectiveness of the frequency of the measurement process.

Objective 5: Financial institution management effectively identifies and implements controls to mitigate identified and prioritized risks associated with the MFS offering.

1. Determine whether management incorporates mobile risks into the overall risk management process.

2. Determine whether management implements policies and procedures for the MFS offering.

3. Determine whether management puts in place appropriate internal controls to ensure security and confidentiality of MFS.

4. Determine whether management implements controls to mitigate all applicable categories of risks related to MFS, including strategic, operational, compliance, and reputation risk.

1. a. Strategic risk mitigation: Review whether management incorporates its decisions to provide MFS into its strategic planning process.

2. b. Operational risk mitigation: Review whether management controls include the following: risk management; transaction monitoring and geolocation tools; fraud prevention, detection, and response programs; additional controls (e.g., stronger authentication [85] and encryption); authentication and authorization processes (e.g., processes to enroll customers and devices in the mobile channel); application development and distribution controls (e.g., process for approving and submitting mobile application code to distribution partners); application security controls (including strategy to deactivate older application versions); contracts and agreements; customer awareness processes; and logging and monitoring processes. Specifically, review the controls that management has in place over the technologies employed for MFS, including the following:

- SMS technology.
- Mobile-enabled Web sites.
- Mobile application.
- Mobile payments.

1. c. Compliance risk mitigation: Review whether management consults with compliance staff, reassessing current mobile service offerings regularly and examining for compliance with applicable laws and regulations.

2. d. Reputation risk mitigation: Review whether management includes the use of controls to minimize or prevent disclosure of personal information and the potential for fraudulent transactions. Also, review management's mitigation of risks associated with the use of a third party, if applicable.

1. 5. Determine whether management has appropriate and independent testing of controls for effectiveness.

Objective 6: Financial institution management maintains effective oversight of MFS

activities. Management maintains appropriate reporting for various levels of management to support that oversight.

1. Review the monitoring process to determine whether the institution has appropriate performance monitoring systems to allow management to assess whether the product or service is meeting operational expectations. Determine whether the systems include the following features:

1. a. Limits on the level of acceptable risk exposure that management and the board are willing to assume.
2. b. Specific objectives and performance criteria to evaluate success of the product or service.
3. c. Ability to produce reports that periodically compare actual results with projections and qualitative benchmarks that provide trend information.
4. d. Ability to produce reports that provide data, which would trigger changes in the business plan, as appropriate.

1. 2. Determine whether the institution's reporting process describes the following:

1. a. MFS activities.
2. b. Information to meet the needs of the various levels of management.
3. c. Trends, volumes, and changes in activity over time.
4. d. Statistics on demographics and locations served to evaluate whether the institution is meeting its strategy.

Objective 7: Discuss corrective action and communicate findings.

1. Review preliminary conclusions with the examiner-in-charge (EIC) regarding the following:

1. a. Violations of laws and regulations.
2. b. Significant issues warranting inclusion as matters requiring attention or recommendations in the report of examination.
3. c. Proposed URSIT [86] management component rating and the potential impact of the conclusion on composite or other component information technology ratings.

4. d. Potential impact of the conclusions on the institution's risk assessment.

1. 2. Discuss findings with management and obtain proposed corrective action for significant deficiencies.

1. 3. Document conclusions in a memorandum to the EIC that provides report-ready comments for all relevant sections of the report of examination and guidance to future examiners.

4. Organize workpapers to ensure clear support for significant findings by examination objective.