Federal Financial Institutions Examination Council

FFIEC

Retail Payment Systems

RPS

MARCH 2004

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 (TSP) on identifying and controlling information technology (IT)-related risks associated with retail payment systems and related banking activities.[1] Financial institutions, either in consortiums or acting independently, remain the core providers to businesses and consumers for most retail payment instruments and services.

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, but increasingly, independent third parties play an important role and financial institution risks are altered if independent third parties are involved. Federal government-affiliated providers and operators, such as the Federal Reserve Banks, also compete with numerous financial institutions and private sector firms in providing various retail payment services.

This booklet replaces chapters 20, "Retail EFT (ATM and POS)," and 21, "Automated Clearing House (ACH)," in the 1996 *FFIEC Information Systems Examination Handbook.* The booklet presents retail payment systems examination guidance in three parts, followed by examination procedures, a glossary, and references.

- *Retail Payment Systems Overview*—The booklet starts with an overview of retail payment systems, grouping retail payment instruments in three categories: checks, card-based electronic payments, and other electronic payments, including person-to-person (P2P), electronic benefits transfer (EBT), and the automated clearinghouse (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. Generic diagrams showing the typical payment flows and clearing and settlement arrangements for each of the retail payment instruments described are also included.[2]

[1] This booklet uses the terms "institution" and "financial institution" to describe an insured bank, thrift, and credit union, as well as technology service providers (TSP) providing services to a financial institution.

[2] 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 http://www.kc.frb.org/FRFS/PSRmain.htm.

- *Retail Payment Systems Risk Management*—The third section describes the risks associated with various retail payment systems and instruments, using the regulatory risk categories including reputation, strategic, credit, liquidity, settlement, legal/compliance, and operational/transaction risk. This section also presents the risk management practices financial institutions should have in place in order to mitigate the risks described and concludes with specific controls appropriate to a number of retail payment instruments. Management action summaries 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." In addition to describing the information technology risks and controls, the booklet also describes 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 might require the use of examiners with experience in credit, liquidity, or compliance issues and additional examination procedures.

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, and 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.

This booklet references specific services and brand names 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.

RETAIL PAYMENT SYSTEMS OVERVIEW

Retail payments usually involve transactions between consumers and 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 payments systems. This section provides background information on payments typically classified as retail payments. Consumers generally use retail payments in one of the following ways:

- *Purchase of Goods and Services*—Payment at the time the goods or services are purchased. It includes attended (i.e., traditional retailers), unattended (e.g., vending machines), and remote purchases (e.g., Internet and telephone purchases). A variety of payment instruments may be used, including cash, check, credit, or debit cards.
- *Bill Payment*—Payment for previously acquired or contracted goods and services. Payment may be recurring or nonrecurring. Recurring bill payments include items such as utility, telephone, and mortgage/rent bills. Nonrecurring bills include items such as medical bills.
- *P2P Payments*—Payments from one consumer to another. The vast majority of consumer-to-consumer payments are conducted with checks and cash, with some transactions conducted using electronic P2P payment systems.
- *Cash Withdrawals and Advances*—Use of retail payment instruments to obtain cash from merchants or automated teller machines (ATMs). For example, consumers can use a credit card to obtain a cash advance through an ATM or an ATM card to withdraw cash from an existing demand deposit or transaction account. Consumers can also use personal identification number (PIN)-based debit cards to withdraw cash at an ATM or receive cash-back at some point-of-sale (POS) locations.

A number of important trends in the past decade have influenced retail payment systems. One such trend is the rapid consolidation of providers of retail payment services. Credit issuers, merchant acquirers, processing companies, and check processors are consolidating as firms seek economies of scale. These changes have meant that some small and mid-sized financial institutions are exiting the business and outsourcing certain functions of the retail payments process to larger financial and nonfinancial institutions.

Another important trend is the shift from paper to electronic payments. Recent research has found that consumer use of electronic payments has grown significantly in recent years, and the trend will accelerate.

Debit and credit cards were one of the key drivers for much of the growth in electronic payments. Although on-line, or PIN-based, debit cards were introduced in the early 1980's, rapid adoption has only occurred since the early 1990's. Off-line, or signature-based, debit cards, introduced in the late 1980's, have experienced significant growth since the mid 1990's, and recent surveys have found that off-line debit card transactions have now overtaken on-line debit card transactions by almost a three-to-one margin.

ACH payments also have grown significantly. Consumers traditionally used checks for a large portion of bill payments in the United States. However, consumers are increasingly using direct bill payment through the ACH. Despite the increase in electronic bill payment, many consumers still rely on checks to make a significant portion of their bill payments. More recently, retail firms have employed check to ACH conversion processes to allow electronic settlement, thus 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 using existing payment systems. Depending on the bill payment software, service provider, and payment receiver used, the payment transaction may be processed as an electronic funds transfer (EFT), ACH, or check.[3]

[3] This booklet addresses the risks and controls associated with the bill payment transaction. See *IT Handbook* "E-Banking Booklet" for the risks and controls associated with the front-end bill payment application used to initiate bill payments.

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.

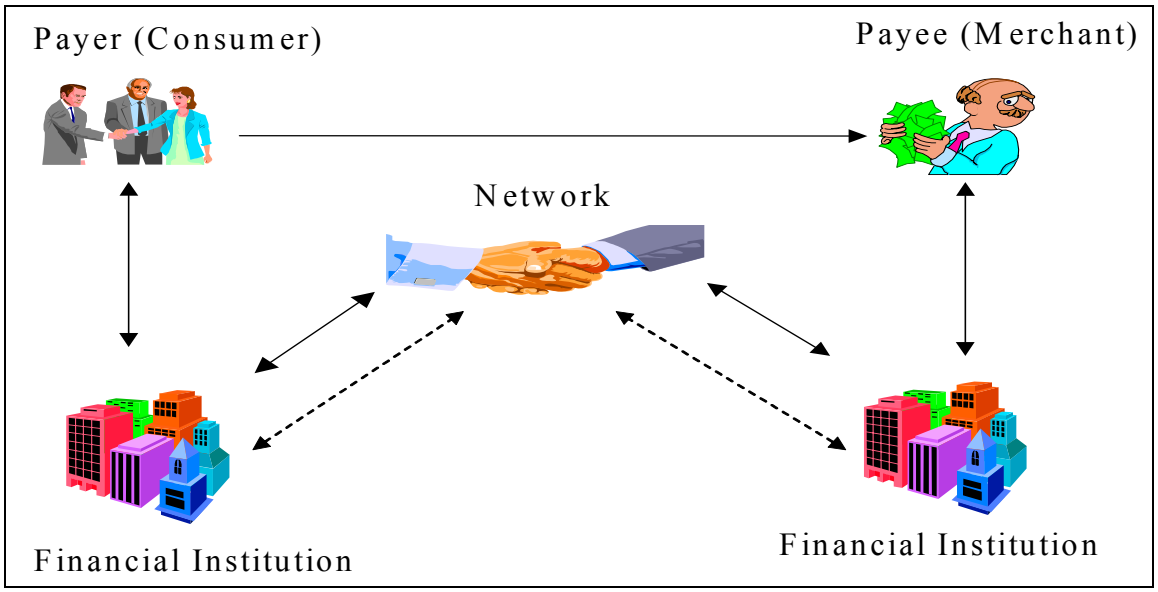


Figure 1: Four-Corner Payments Model

Figure 1 displays the clearing and settlement process for retail payments using a standard four-corner payments model. While the flow of information, data, 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 in retail payments, 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 bottom two corners of the model represent the relationship of the consumer and merchant to their financial institution. In some cases, third-party service providers will act on behalf of financial institutions. The payments networks or clearinghouse organizations that route the transactions between financial institutions are in the middle of the chart. In some instances, for example check clearing, a financial institution may exchange check items directly with another financial institution bypassing the clearinghouse. In figures 1 through 8 solid lines represent the flow of information and dashed lines represent the flow of funds.

CHECK-BASED PAYMENTS

Until recently, consumers used checks more often than any other retail payment instrument in the United States other than cash. Checks are very convenient payment instruments. Consumers can use them at the point of sale, for bill payments, and for person-to-person transactions. Nonetheless, checks comprise a decreasing percentage of the total non cash payment volume in the United States.

In recent years, check-clearing associations, financial institutions, and the Federal Reserve have introduced or participated in various electronic check presentment (ECP), electronic check conversion (ECC), and check imaging initiatives supporting the conversion, or truncation, of checks to electronic form. Consumers will no longer have a float period when using electronically converted checks for purchasing goods and services and paying bills.

ECP improves the speed of collection and return of checks. It enables check truncation by using magnetic-ink character recognition (MICR) line information to present checks electronically to the paying institution for payment. ECP eliminates the need to forward the paper check physically. Check imaging technology supports ECP and the creation and use of "substitute checks" stored on secure electronic media for retrieval when needed.

Increasingly, using ECC, payees convert checks to ACH or EFT transactions. Once the payee converts the check at the point of sale through ACH or EFT, or in a lock box environment through ACH, the transaction is governed by existing regulations for whichever electronic payment network is used.

In the past, financial institutions have agreed among themselves to use various forms of check truncation, such as using a check image or MICR information from a check to substitute for the original check. The Check 21 Act (CTA) declares that a qualifying substitute check shall be the legal equivalent of an original check even in the absence of institution-specific agreements.[4] Such substitute checks must meet certain specified requirements to be treated as a legal equivalent, and the truncating institution must indemnify other parties for losses that result from their receipt of a substitute check instead of the original check. Financial institutions should consider the implications of the CTA on the institution's risk profile. Examiners should stay current with anticipated supervisory guidance that will address the significant risks that can arise from implementation of the CTA.

[4] See BAI for further information at http://www.bai.org/check21/.

CHECK CLEARINGHOUSES

A check includes the names of the payer and the payee, the account number, amount of the check, and the name of the paying financial institution. The 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).[5]

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

Under direct presentment, depositary financial institutions can present checks directly to the paying financial institution. The paying financial institution may settle with the depositary financial institution through a pre-arranged settlement agreement or settle by sending Fedwire® funds transfers through the Federal Reserve Banks.[6]

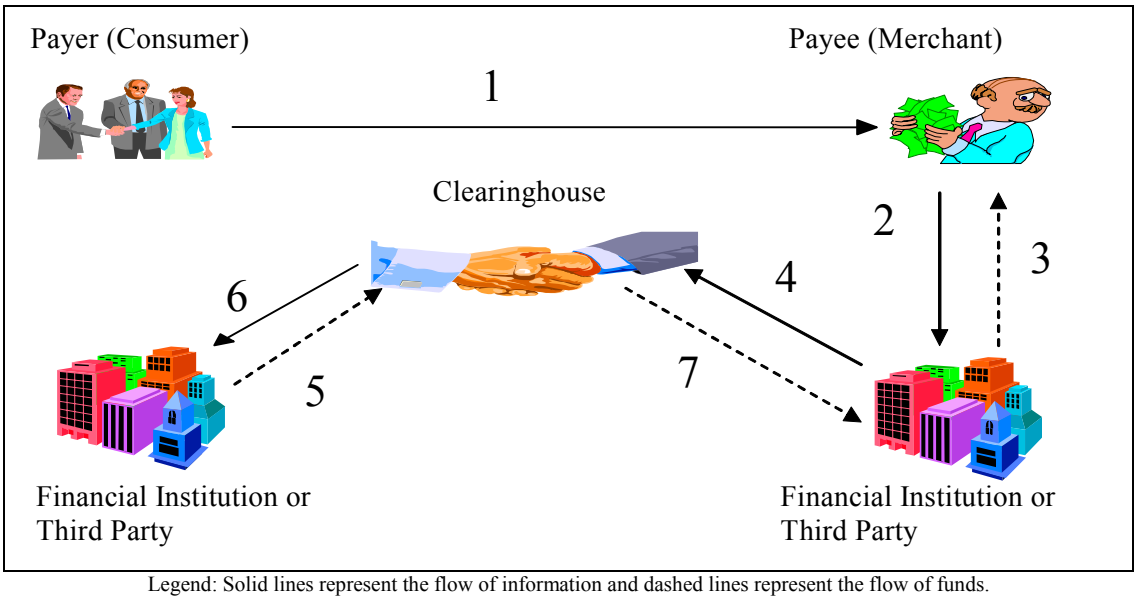
Correspondent banks, acting on behalf of other depository financial institutions, can settle the checks they collect for other institutions, known as respondents, by using accounts on their books or using their Federal Reserve Bank reserve account.

Financial institutions can also clear checks through a Federal Reserve Bank or an independent clearinghouse, where they have formed voluntary associations that establish an exchange for checks drawn on those financial institutions. Typically, financial institutions participating in check clearinghouses use the Federal Reserve's National Settlement Service to effect settlement for checks exchanged each business day.[7] There are approximately 150 check clearinghouse associations in the United States. Smaller depository institutions typically use the check collection services of correspondent banks or the Federal Reserve Banks.

[5] See http://www.ansi.org/.

[6] See *IT Handbook* "Wholesale Payment Systems Booklet" for a discussion of Fedwire®.

[7] See http://www.frbservices.org/Wholesale/natsettle.cfm.



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 Federal Reserve Bank or clearinghouse. In step 1 the consumer uses a check to pay a merchant for goods or services. The merchant, after authorizing the check, accepts the check for payment.[8] 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 immediately available. For deposited checks payable at other financial institutions, the merchant's financial institution uses direct presentment for processing or sends the checks to a Federal Reserve Bank, clearinghouse, or correspondent bank (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, clearinghouse, or Federal Reserve Bank is debited (steps 5 and 7).[9]

CARD-BASED ELECTRONIC PAYMENTS

A variety of electronic payments are available for retail use. Some are card-based, while others are electronic instructions for funds transfers. Usually, these payments link to an existing account relationship with a financial institution for both payee and payer.

Consumers may use credit, debit, or stored-value cards to initiate retail payments in face-to-face or remote transactions. The payee receives funds after the payment clears, but consumers actually pay before the transaction on a stored-value card, at the same time of

[8] Check authorization is typically performed by a TSP and can also include ECC and other electronic payment services.

[9] Under CTA, the original or a qualifying substitute check is needed for presentment unless agreed to otherwise.

the transaction for an on-line debit card, and after a transaction on a credit card. Both credit 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, although processed in real time at the POS, typically settle at the end of the day using the ACH. Each of these types of card payments is described below.

CREDIT AND CHARGE CARDS

Financial institutions are important participants in various credit card systems. They issue and distribute cards, clear and settle the associated payments, and in some cases act as merchant acquirers. Credit cards can have revolving credit arrangements, and charge cards have a short-term, fixed-period, credit arrangement. Revolving credit arrangements allow customers to 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. With charge cards, the consumer must fully pay the outstanding balance at the end of the one-month charge or billing period. This arrangement exposes the issuing institution to less credit risk than open-ended accounts.

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 are cards that have the logo of one of the bankcard associations on the front. These cards have an associated account at a financial institution or other business with a credit line that limits the value of outstanding payments. They can be used at any location that accepts cards from the particular card association. General-purpose credit cards 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 two major credit card associations, Visa and MasterCard. The bankcard associations operate "open" networks in which financial institutions can compete in card issuing and merchant acquiring. The card-issuing financial institution and merchant acquirer can be different organizations.

- Firms that serve as both the card-issuing agent and the merchant acquirer issue *closed-loop credit cards.* They issue the cards in conjunction with specific non-bankcard brand names including American Express, Discover, and Diner's Club.

Co-Branded/Affinity Credit Cards

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

Companies with which the cardholder has a relationship issue co-branded cards jointly with specific financial institutions. They typically offer consumers some kind of rewards program. Organizations such as sports teams, schools, or service organizations issue affinity cards jointly with a financial institution which offers compensation in return for marketing to the merchant's customers or the organization's members. The institution can 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 private label or store cards. Consumers can only use them at the merchant whose name appears on the front of the card. These cards do not carry a bankcard association logo, and the merchant typically plays a limited role in the issuance of the card or managing the credit relationship.[10]

BANKCARD ASSOCIATIONS

The two major bankcard associations, Visa and MasterCard, in conjunction with credit card issuing and acquiring financial institutions, account for the majority of credit and debit cards in use. Both associations began as bank service companies, owned by principal member financial institutions. They provided uniform operating policies, procedures, and controls for bankcard issuance, acquiring, and settlement activities. The associations own the credit card trademark, granting membership to financially sound institutions that apply. The associations only allow members to issue cards bearing the association logo. Members pay transaction and membership fees for use of the bankcard association logo and services.

Both associations have three types of membership: principal, associate (VISA)/affiliate (MasterCard), and participant (VISA)/agent (MasterCard). 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 association. Associate/affiliate and participant/agent

[10] Certain private label (store) credit card retailers actively manage card issuance and credit relationships through affiliated financial institutions.

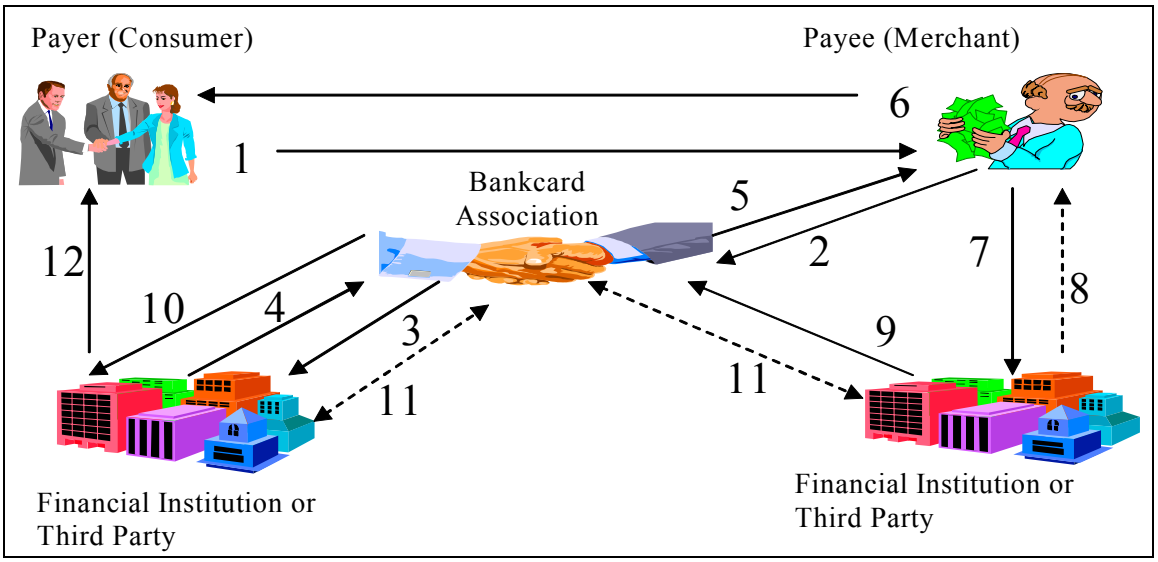
members can perform all of the principal membership functions except sponsor other members.

The closed-loop credit card networks—American Express, Discover, and Diner's Club—compete with the major bankcard associations to promote the use of their cards. However, in the case of the closed-loop credit card networks, the card issuer and merchant acquirer are the same financial institution.

Card-issuing institutions are financial institutions that have permission to issue bankcard association credit cards. Acquiring financial institutions and third parties have contracts with merchants that accept a bankcard association's products. The financial institutions accept and process transactions from those merchants through the association's network interchange payment system. The cost of technology infrastructure and level of transaction volume are high for bankcard-acquiring institutions. Most rely on third-party processors to perform the functions.[11] Under the bankcard association bylaws, acquiring financial institutions are responsible for the actions of all contracted third-party processors, and therefore are expected to carefully monitor service provider compliance with the associations' operating rules.

The bankcard associations 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 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., chargeback processing and account maintenance) they charge to the merchant.

11 Non financial institution processors must partner with financial institutions to process merchant transactions.



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

Figure 3: Credit Card Clearing and Settlement

Figure 3 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, through the bankcard association'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). 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 association, who in turn forwards the data to the card issuer (steps 9 and 10). The bankcard association determines each financial institution's net debit position. The association's settlement financial institution coordinates issuing and acquiring settlement positions. Members with net debit positions (generally issuers) send owed funds to the association's settlement financial institution, which transmits owed funds to merchant acquirers. The settlement process takes place using a separate payment network such as Fedwire® (step 11).[12] 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.

[12] 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.

DEBIT AND AUTOMATED TELLER MACHINE (ATM) CARDS

Debit cards are associated with an existing transaction account at a financial institution. The card enables consumers to access the account for a variety of transactions. Debit cards are either on-line (e.g., PIN-based) or off-line (e.g. signature-based). On-line debit cards have been available for several decades and have seen tremendous growth since the early 1990's. Off-line debit cards are a more recent innovation and consumers are increasingly using them at merchant locations that accept bankcards.

- *On-line debit cards* use a PIN for customer authentication and on-line access to account balance information. In the future, consumer authentication could also occur through the use of some other technology, such as a biometric indicator. At present, financial institutions authenticate customers by matching the PIN with the account number directly through a merchant's terminal. Debit card transactions use the same EFT networks that handle ATM transactions. Customers may also receive cash at the POS because messaging between the financial institution and the retailer confirms funds availability.

- *Off-line debit cards* authenticate consumers through a written signature or other authenticating action. Introduced in the late 1980's by Visa and MasterCard, use of off-line debit cards has grown tremendously. The transactions process through the same bankcard networks as credit card transactions and typically settle at the end of the business day. A cardholder can generally use an off-line debit card anywhere that accepts a similarly branded credit card, although the cardholder cannot receive cash back at the POS. A hold is placed on the cardholder's funds, effectively lowering the available balance in their transaction account, but there is no real time connection that guarantees the availability of funds. See figure 3.

As a result of a legal settlement with Wal-Mart and other retailers, beginning in 2004, merchants will no longer be required to accept Visa and MasterCard off-line debit cards as a condition for accepting bankcard associations' branded credit cards. This is a dramatic change from the longstanding "honor all cards" policy previously established by the bankcard associations used to enhance merchant acceptance of off-line debit. How this policy change will affect the popularity and profitability of off-line debit cards with merchants and cardholders is uncertain.

ATM Cards

Financial institutions issue ATM cards to consumers to provide on-line 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 retailers.

EFT/POS NETWORKS

EFT/POS networks process, route, clear, and settle ATM and on-line POS debit card transactions by linking financial institution card issuers and merchant acquirers, consumers, merchants, and third-party service providers through telecommunication gateways. The networks' primary roles include routing transactions through central switching gateways, acting as clearinghouses to settle network member "on-us" transactions, and forwarding "foreign" nonmember transactions for processing.

Most financial institution and nonbank ATM networks are connected to regional and national EFT/POS networks. Most regional networks are joint ventures owned and controlled by competing financial institutions. Ownership in regional networks can either be concentrated in several financial institutions or dispersed among 100 or more member financial institutions. A few regional networks function as cooperatives, while a single firm may own and operate one as a profit-making enterprise.

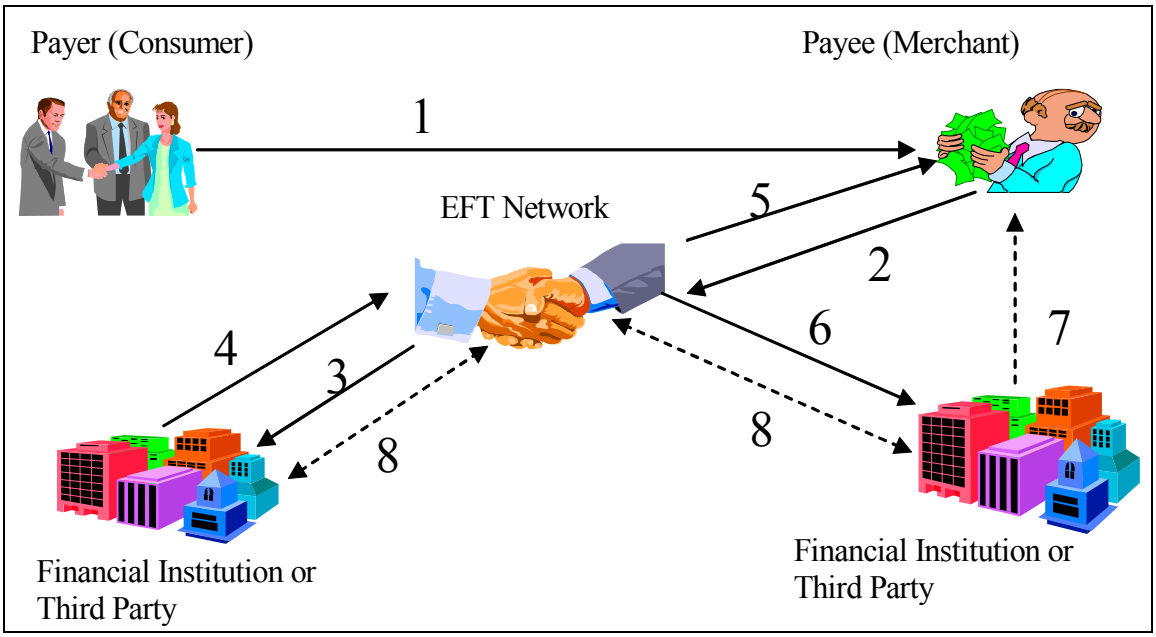
Visa and MasterCard own and operate the two national EFT/POS networks: Visa's Plus and MasterCard's Cirrus ATM networks and Visa's Interlink and MasterCard's Maestro POS networks. These national networks serve as a bridge between regional networks, and permit transaction information to be routed from one regional network to another.

Membership in regional and national EFT/POS networks facilitates universal access to financial institution card-based electronic services, providing participant financial institutions with an interchange system offering authorization, clearing, and settlement services. The fees financial institutions charge consumers for "foreign" ATM usage help defray the cost of membership services. Acquirers collect interchange fees from network members (issuers) to cover the cost of operations. With ATM transactions, the issuer pays the acquirer, in contrast to credit and debit card networks. EFT/POS networks clear both ATM and debit card (PIN-based) transactions.

Financial institutions rely on third-party service providers to conduct ATM and debit card payment processing. Third-party processors provide a range of retail payment-related

services, including card issuing services, merchant services, account maintenance and authorization services, transaction routing and gateway services, off-line debit processing services, and clearing and settlement services. Although merchant acquiring financial institutions may use third parties to perform many acquiring activities, the acquiring financial institution is responsible for all third-party processor and merchant activity.

Independent sales organizations (ISO) 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 processors for a variety of services including ATM and POS terminal driving, 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 4: PIN-based Debit Clearing and Settlement

Figure 4 describes a generic, on-line, 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 (steps 2 and 3). The consumer's financial institution, or in some cases the regional network, verifies funds and debits the consumer's account (step 4). The EFT/POS network contacts the merchant and authorizes the purchase (step 5). For settlement, 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 6).

The acquiring financial institution typically does not credit the merchant's 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

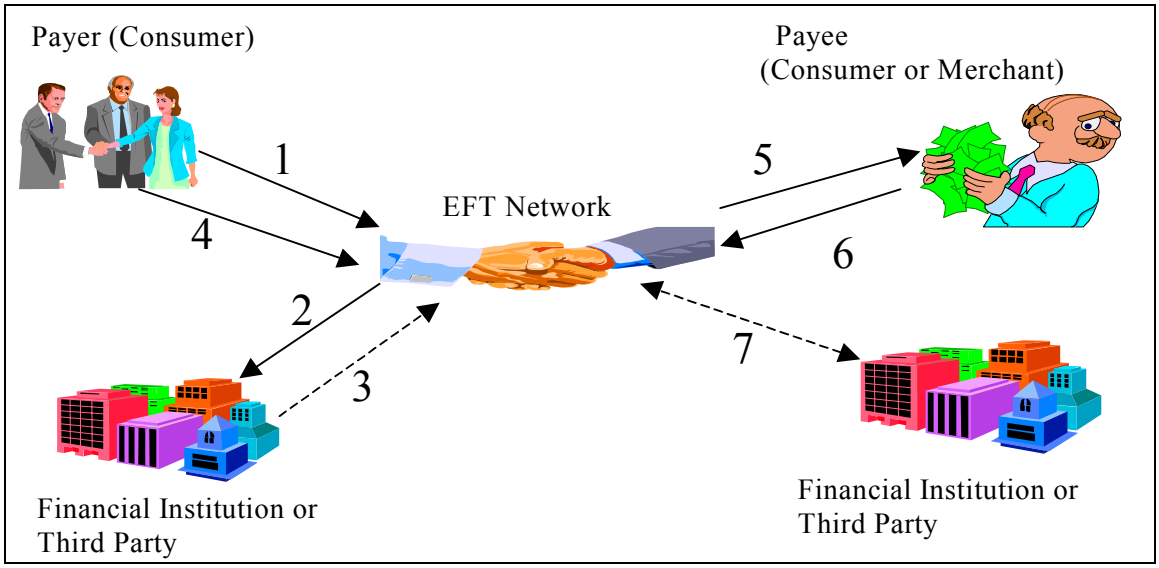
acquiring financial institution and other intermediaries to the transaction (step 7). At the end of the business day, the issuing and acquiring financial institutions establish a net settlement of all the transfers between them using the ACH (step 8).

STORED VALUE CARDS

Financial institutions and nonfinancial businesses issue stored value cards. Either the consumer or the issuer funds the account for the card. Generally, the issuer does not pay interest on the card balances. When a consumer uses the card to make a purchase, the merchant deducts the amount of the purchase from the card. Once they exhaust the stored value in the card, customers may either replenish the value or acquire a new card. Transaction authorization can take place through an existing network, a chip stored on the card, or information coded on a magnetic strip. These cards are typically used for low-value purchases.

Stored value cards, mostly issued by nonfinancial businesses, have been successful in limited deployment environments such as mass transit systems and universities. In addition to cards, nonfinancial businesses have introduced a variety of other physical forms for carrying the customer account information. These physical devices are small and easily portable (e.g., key fobs, rings, etc.)

Some stored value cards may also be smart cards if they contain an integrated microchip. The integrated chip can store value and perform other functions, such as consumer authentication. The chip can be placed on a stored value card, a credit card, or a debit card. The chip might also contain consumer preferences and loyalty program information for marketing purposes.



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

Figure 5: Stored Value Card Clearing and Settlement

Stored value card transactions typically follow the pattern in figure 5. The consumer purchases a stored value card (steps 1 and 2). When the consumer pays for goods or services with a "smart" stored value card, electronic notations or tokens transfer from the card to the merchant's cash register (steps 3, 4, and 5). The merchant contacts the computer network of the financial institution that issued the stored value 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 institutions keep a percentage of the payment (the discount) as compensation for the services provided.

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

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

OTHER ELECTRONIC PAYMENTS

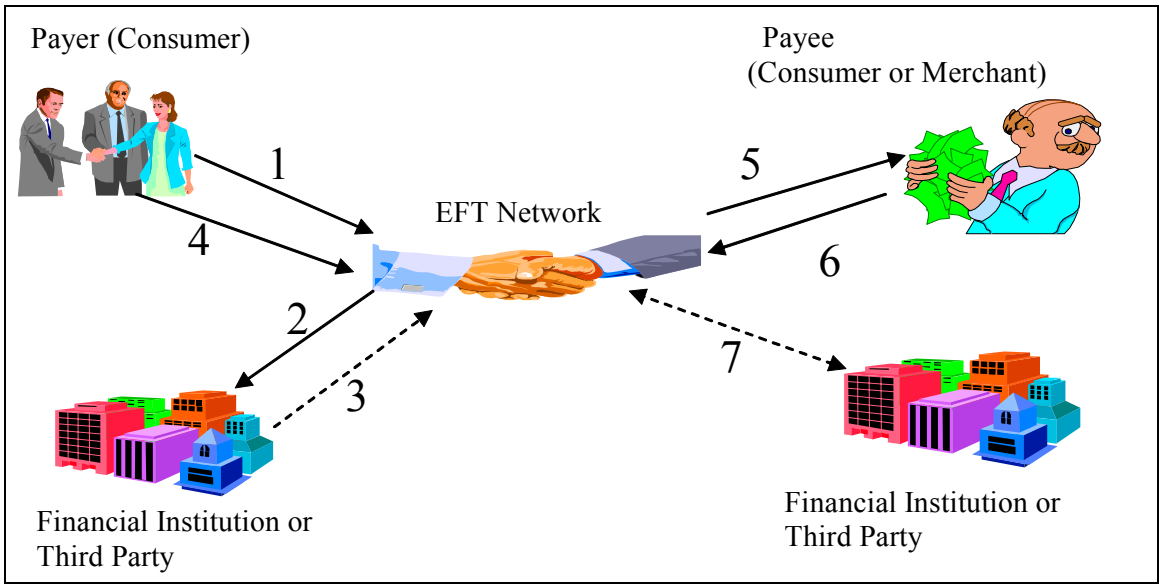
Other electronic payments include P2P payments, electronic cash, and electronic benefits transfer (EBT). These payment instruments are usually associated with an established consumer deposit account and facilitate consumer access to recurring and one-time debit and credit transactions and a variety of federal, state, and local government benefit programs.

ON-LINE P2P PAYMENTS AND ELECTRONIC CASH

On-line P2P payments, or e-mail payments, use existing retail payment networks to provide an electronically initiated transfer of value. An individual can send a payment to another individual by entering the desired amount and the recipient's e-mail address. Though these payments are named for their ability to send funds among individuals on-line, the majority of P2P payments are Internet purchases at on-line auctions or small businesses. In most cases, P2P transfers use existing retail payment systems to add and withdraw funds from accounts. The transfer of value between individuals occurs using proprietary networks as "on-us" transactions.

Most P2P services charge the receiver of the funds a variable fee depending upon various factors, including payment method and the sender's credit history. Payments made with funds that originated from an ACH transaction are less expensive than transactions made

with funds originated from credit cards. P2P systems may offer the receiver an opportunity to obtain funds through a check for an additional fee.



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

Figure 6: On-line P2P Clearing and Settlement

On-line P2P payments typically occur using the process described in figure 6. 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 be drawn from a previous balance with the on-line P2P payment provider (steps 2 and 3). The sender can then designate the e-mail address of the intended funds recipient (step 4). The P2P network then 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 on-line P2P payment service can disburse the funds from the receiver's P2P account through an ACH payment, a check payment, an EFT credit, or a credit to a credit card account (step 7).

Electronic Cash

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. Most electronic cash applications exist on 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. Prefunded accounts consumers may use for on-line auction payments or with participating retailers are among the most recent applications. Individuals use a credit card or signature-based debit card number to prefund the Web certificate or electronic account, and recipients redeem the

value with the issuer. There are few existing markets for electronic cash payment instruments, and merchant acceptance and consumer use is generally low.

ELECTRONIC BENEFITS TRANSFER (EBT)

EBT systems allow government benefits recipients 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 nearly 80 percent of 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.

THE AUTOMATED CLEARINGHOUSE (ACH)

The operating rules of the National Automated Clearinghouse Association (NACHA) govern ACH transactions.[13] ACH transactions are payment instructions to either debit or credit a deposit account. An ACH transaction is a batch-processed, value-dated electronic funds transfer between originating and receiving financial institutions. ACH payments can either be credits, originated by the accountholder sending funds (payer), or debits, originated by the accountholder receiving funds (payee). Financial institutions may contract with third-party service providers to conduct their ACH activities, and independent third parties not affiliated with financial institutions now generate significant ACH payment activity.

ACH payments are used in a variety of payment environments. Originally, consumers primarily used the ACH for paycheck direct deposit. Now, they increasingly use the ACH for bill payments (often referred to as direct payments), corporate payments (business-to-business), and government payments (e.g., tax refunds).

In addition to the primary ACH transactions, retailers and third parties use the ACH system for other types of transactions including:

- *Electronic check conversion.* Electronic check conversion is the process of transmitting MICR information from the bottom of a check through the ACH. Its most common application is with checks drawn on consumer accounts. Some retailers and third-party providers have been converting checks to ACH transactions at the point of purchase. In addition, some corporations and financial institutions use it to convert check payments to ACH items at lock box locations.

[13] See http://www.nacha.org/.

- *Internet-originated and telephone-initiated ACH payments.* Consumers and retailers can initiate ACH transactions over the telephone and Internet. These ACH transactions are an alternative to providing a credit card or signature-based debit card number. In addition, retailers do not pay an interchange fee for ACH transactions.

THE ACH NETWORK

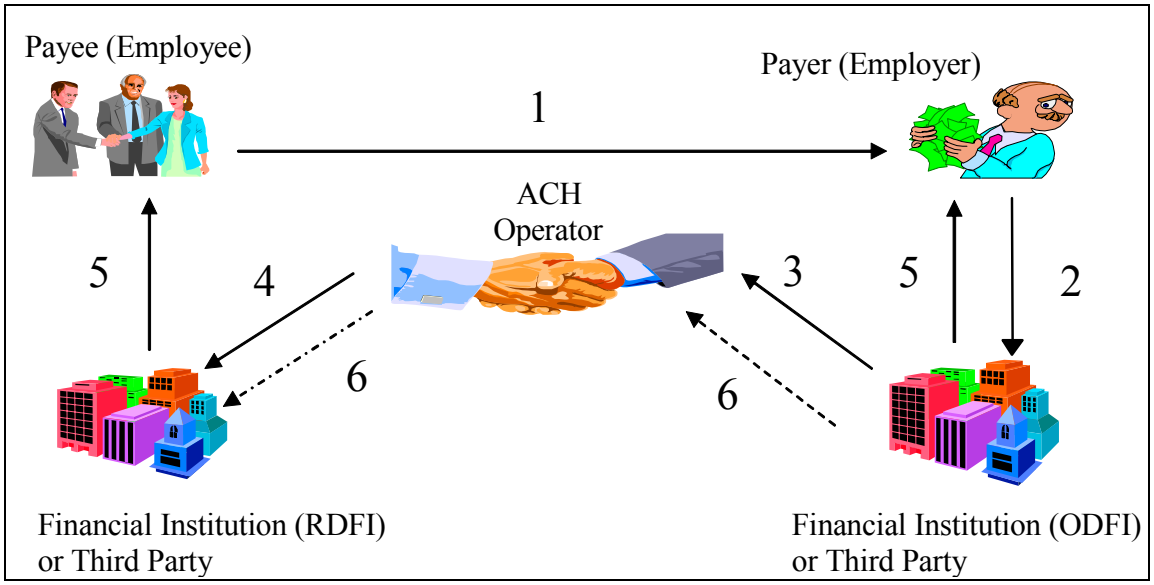
ACH transactions are sent in batches to ACH operators for processing one or two business days before settlement dates. The ACH operators deliver the transactions to the receiving institutions at defined times. There are two national ACH operators. The Electronic Payments Network (EPN) is a private processor with approximately 30 percent of the national market as of the end of 2002.[14] The Federal Reserve Banks process the remaining share of the market. ACH operators charge a small per-transaction fee 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 and transaction instructions and funds are linked using codes for record keeping. If the ODFI sends funds, it is a credit transaction. Examples of credit payment transactions include payroll direct deposit, Social Security payments, and dividend and interest payments. Corporate payments to contractors, vendors, or other third parties are also common ACH credit transactions. 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.

Financial institutions originating customer payments have a binding commitment for payment to the ACH operator when the ACH files are distributed. Settlement for Federal Reserve Bank ACH credit transactions is final at 8:30 a.m. Eastern Time (ET) on the settlement day, when posted to depository financial institution accounts. Settlement is final for ACH debit transactions when posted at 11:00 a.m. ET on the settlement day.[15]

[14] EPN is a subsidiary of The Clearing House (formerly known as the New York Clearing House Association).

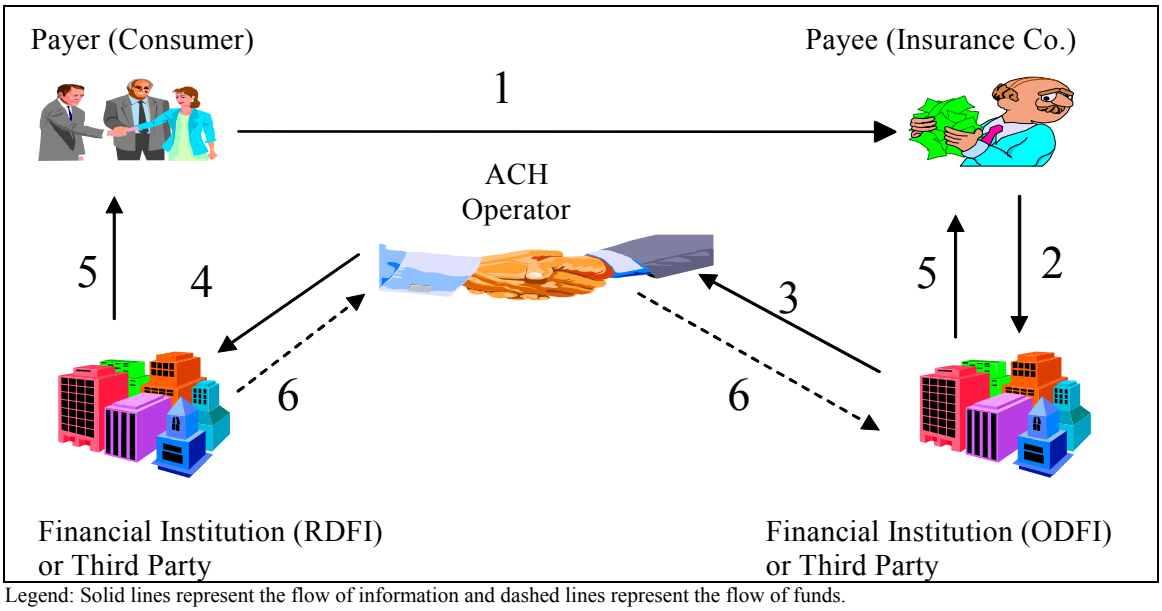
[15] See http://www.frbservices.org/OperatingCirculars/pdf/oc4.pdf for Federal Reserve System Operating Circular No. 4 on "Automated Clearing House Items."



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

Figure 7: ACH Credit Clearing and Settlement

Figure 7 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 financial institution makes the funds available to the payee by crediting his or her account and debiting the payer's account (steps 4 and 5). The ACH operator settles the transaction between the participating financial institutions (step 6). If the ACH operator is the EPN, final settlement is done using the Federal Reserve Bank's National Settlement Service (NSS). If the ACH operator is the Federal Reserve, final settlement is made directly to the financial institution's reserve accounts at a Federal Reserve Bank.



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

Figure 8: ACH Debit Clearing and Settlement

Figure 8 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 7.

PAYMENTS SYSTEM RISK (PSR) POLICY

Similar to financial institutions offering retail payment services to customers, the Federal Reserve Banks are exposed to credit risk when they process payments for financial institutions holding reserve accounts. The Federal Reserve Banks guarantee payments for financial institutions using their systems for Fedwire® Funds, NSS, and ACH credit originations. Due to this payment guarantee, the Federal Reserve Banks may incur losses when institutions fail with overdrafts in their accounts.

The Federal Reserve's Payments System Risk (PSR) policy controls and reduces intraday credit risk to the Federal Reserve Banks.[16] An integral component of the PSR policy is a program to control the use of Federal Reserve daylight overdrafts. Daylight overdrafts can occur in accounts at Federal Reserve Banks as well as at financial institutions. A daylight overdraft occurs at a Federal Reserve Bank when there are insufficient funds in

[16] See http://www.federalreserve.gov/paymentsystems/psr/default.htm.

an institution's Federal Reserve account to cover outgoing Fedwire® funds transfers, incoming book-entry securities transfers, or other payment activity processed by a Federal Reserve Bank.

To control daylight overdrafts, the PSR policy establishes limits, or net debit caps, on the amount of Federal 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 sufficiently flexible to reflect the overall financial condition and operational capacity of each institution using Federal Reserve Bank payment services. The policy also permits the Federal Reserve Banks to protect themselves from the risk of loss by unilaterally reducing net debit caps, imposing collateralization or clearing-balance requirements, rejecting or delaying certain transactions until sufficient balances exist, or prohibiting an institution from using Federal Reserve payment services.

The PSR policy established daylight overdraft fees to provide a financial incentive for institutions to control their use of Federal Reserve Bank intraday credit and to recognize the risks inherent in the provision of intraday credit. Daylight overdraft fees induce financial institutions to make business decisions concerning the amount of Federal Reserve Bank intraday credit they are willing to use based on the cost of using that credit. The daylight overdraft measurement method, which incorporates a set of nearly real time transaction posting rules, also supports institutions in controlling their use of Federal Reserve Bank intraday credit.

The Federal Reserve Banks use the real time Account Balance Monitoring System (ABMS) to monitor financial institution accounts intraday. For a limited number of institutions, the system is used to prevent them from incurring daylight overdrafts in their Federal Reserve Bank accounts beyond a certain threshold (often set to zero) for Fedwire® Funds, NSS, and ACH credit origination transactions. This is referred to as monitoring the account in real time.

The Federal Reserve Banks require prefunding for any ACH credit origination transactions settling to the accounts of financial institutions that are monitored in real time. ACH transactions for accounts that are monitored in real time are also required to be prefunded on behalf of the account holder and any respondents.

Institution accounts that are monitored in real time must have sufficient available funds when they process ACH batches that contain forward credit items (credit or mixed batches with debit and credits). If there are insufficient funds available in the account, the batch will reject and a notice will be sent to the ACH sending point and to the settlement financial institution.[17]

[17] See *IT Handbook* "Wholesale Payment Systems Booklet" for additional information on NSS and PSR policy.

RETAIL PAYMENT SYSTEMS RISK MANAGEMENT

Action Summary

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

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 clearance and settlement systems. Institutions must comply with federal and state laws as well as with clearinghouse, bankcard association, and regulatory requirements associated with retail payment transactions.

From the initiation of a retail payment transaction to its settlement, financial institutions are exposed to certain risks. For individual retail payment transactions, risk resulting from compliance issues and potential operational failures, including fraud, is 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 risk may be interdependent with payment system operators and third parties.

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

- Understand the financial institution's practices and controls regarding the risks of processing large-dollar transactions for both its own account and the accounts of its customers or respondents,

- Establish prudent limits on the daylight overdraft or net debit position that the financial institution may incur in its Federal Reserve Bank reserve account or private-sector clearing and settlement systems, and

- Review periodically the institution's daylight overdraft activity to ensure the institution operates within the established guidelines.

The failure of any payment system participant to provide funding for settlement may precipitate liquidity or credit problems for other participants, regardless of whether they were party to payments to or from the failing participant. Operational and credit risk can also contribute to legal (compliance) risk if financial institutions do not follow prescribed regulations and clearinghouse and bankcard association rules and bylaws. In addition, financial institutions have significant reputation risk if they do not correct deficiencies.

Risk profiles vary significantly based on the size and complexity of the financial institution's retail payment system products and services, information technology 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 they offer. Effective internal controls should include the financial, accounting, technical, procedural, and administrative controls necessary to minimize risks in the retail payment transaction, clearing, and settlement process. These measures reduce operational and credit risks, ensure individual transactions are valid, and mitigate processing and other errors. Effective controls also ensure supporting information technology systems 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. Even newer, Internet-based, electronic services have substantial credit and operational risks. Financial institutions should be cognizant of the reputation and strategic risk of newer 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.

Financial institutions have always offered a variety of retail payment services. Advances in information technology continue to expand the variety of services. The industry trend is moving from traditional paper-based transactions to all-electronic transaction services. The newer electronic services increasingly rely on information and network technology, which require financial institutions to develop strong risk management practices.

Financial institutions should establish internal risk management systems that are commensurate with the size and complexity of their operations. The systems should be

capable of evaluating operational risk exposure and the effectiveness of current controls.[18]

STRATEGIC RISK

Strategic risk is the risk associated with the financial institution's future business plans and strategies. 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 and information technology and networking). Financial institutions also increasingly compete with nonbank entities to provide retail payment services. This competition benefits the consumer through enhanced product offerings at a lower cost. Conversely, it 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 may expose financial institutions to increased risk. 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. Strategic plans should demonstrate that management has assessed the risks and documented the institution's program to mitigate them. Strategic plans should address the institution's capability to provide the service.

Larger financial institutions often specialize in specific retail payments and invest in the resources and expertise to support high-volume transaction processing applications. Smaller financial institutions also compete in some retail payment segments through the use of advanced distributed information technology platforms and third-party service providers. Many retail payment system services are transaction intensive and priced competitively based on volume. Financial institutions providing large-scale bankcard issuing and merchant services, as well as other transaction-intensive retail services, should maintain a competitive operating environment. This often requires significant investments in information technology. Strategic plans should reflect these investments and link business-line goals and objectives with planned information technology enhancements.

To mitigate strategic risk, management should have a strategic planning process that addresses its retail payment business goals and objectives, including supporting information technology components. Because financial institutions often rely on third-party service providers for retail payment system products and services, the strategic plan should include a comprehensive vendor management program.

[18] As proposed under Basel II, financial institutions might need to quantify operational risk.

REPUTATION RISK

Reputation risk is the risk that negative publicity regarding an institution's business practices will lead to a loss of revenue or litigation. For retail payment-related systems, reputation risk is linked with customer expectations regarding the delivery of retail payment services, and whether the institution is meeting its regulatory and consumer protection obligations relating to those services. An institution's reputation, particularly the trust afforded it by customers and counter-parties can be irrevocably tarnished due to perceived or real breaches in its ability to conduct business securely and responsibly. In addition, financial institutions are responsible for risks associated with the activities of third-party service providers with which they contract. For example, deficiencies in security and privacy policies that result in the release of customer information by a service provider may result in reputation damage.

CREDIT RISK

Credit risk is the risk that 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, it 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 their accounts to settle transactions.

Non-cash retail payments, including the inter-institution settlement of cash withdrawals through shared ATMs, are usually settled on a deferred basis. With the deferred settlement, there is a risk that the paying institution or some intermediate party will fail before inter-institution settlement occurs. This deferred settlement, rather than real time settlement, mitigates but does not eliminate the credit risk.

When an institution supplies funds, it usually does not submit a payment for settlement unless the payer's financial institution verifies that funds are available in the payer's account. Otherwise, there is a credit risk exposure. When an institution receives funds in a retail payment transaction, it may suffer credit risk from granting funds availability for account transfers not properly authorized. In the ACH, NACHA has established rules requiring each ODFI to conduct appropriate creditworthiness monitoring, establish exposure limits, and periodically review the limits applicable to specific customers.

Returns are another source of credit risk. Checks and direct debit transfers can be returned if the payer's institution chooses not to honor the presentment because of insufficient funds, forgery, fraud, or other payment irregularities. The return time frames 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 under NACHA rules extends to 60 days from the settlement date.

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. In principle, 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 only at some unspecified time in the future. Liquidity problems can result in opportunity costs, defaults on other obligations, or costs associated with obtaining the funds from another

source for some period 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 is the risk arising from failure to comply with statutory or regulatory obligations. Legal risk also arises if the rights and obligations of parties involved in a payment are subject to considerable uncertainty, for example if a payment participant declares bankruptcy. 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 can also potentially cause systemic risk to the payments system. Such legal problems are more likely to result from the failure of a financial institution than the default of an individual payer. Individual default is more prevalent and has often been addressed in existing law.

Legal risk can result from a financial institution's failure to comply with the bylaws and contractual agreements established with the bankcard associations, clearinghouses, and other counter-parties with which it participates in processing, clearing, and settling retail payment transactions.

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 (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 this customer information.

Legal measures should ensure compliance with specific laws and regulations pertinent to retail payment systems. They should also ensure compliance with general consumer protection rules that allocate responsibility and establish the minimum procedural measures that must be fulfilled before shifting the responsibility to another party. 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.

The bylaws and agreements between clearinghouse participants and bankcard associations include specific responsibilities and liabilities. Financial institutions should assess the risks of agreeing to such bylaws and agreements. Financial institutions and third-party service providers that do not comply with the appropriate bylaws and agreements of bankcard associations and clearinghouses can be fined or lose their memberships.

Patriot Act

The USA Patriot Act contains measures to prevent, detect, and prosecute terrorism and international money laundering. Such acts may be perpetrated using retail payment systems. These acts may occur in many ways, including those in which a financial institution does not properly authenticate its accountholders for retail payment transactions. Title III of the USA Patriot Act amends the Bank Secrecy Act and provides the Treasury Department and federal agencies with enhanced authority to combat international money laundering and block terrorist access to the U.S. financial system. Sections 311, 312, 313, 314, and 319 generally require U. S. financial institutions to establish appropriate and, if necessary, enhanced due diligence procedures to detect and report instances of money laundering and terrorist activity.[19] In addition, section 326 requires financial institutions to document authentication of various payment accounts and maintain that documentation.

OPERATIONAL (TRANSACTION) RISK

Operational risk is the risk of incurring financial loss due to human or technical errors and fraud. Operational risk can arise from the failure to follow or complete one or more steps in the prescribed authorization process. Operational risk includes the risks associated with the failure of communications, the breakdown of data transport or processing, internal control system deficiencies, human errors, or management failure. 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. A financial institution's exposure to operational risk from fraud is the risk that a wrongful or criminal deception will lead to a financial loss for one of the parties involved. Currency and checks are more vulnerable to loss or direct theft, whereas fraud is the primary concern in bankcard payment transactions. Fraud is a significant concern for ACH, especially one-time ACH debit transactions. The continuing growth of check-to-ACH conversion presents many new fraud risks.

Newer retail payment mechanisms, particularly using the Internet, are also subject to fraud risk. The creation of fraudulent electronic transactions could lead to financial losses if fraudulent balances are successfully exchanged for a readily transferable form of money, such as currency, or other assets.

Operational risk controls should include information system, procedural, administrative, and legal measures to prevent or limit financial loss as a result of operational risk.

[19] See *IT Handbook* "Wholesale Payment Systems Booklet" for additional information. FFIEC agencies have revised their Bank Secrecy Act (BSA) examination procedures to reflect the USA Patriot Act.

System measures include monetary and time limits (per transaction, per payment instrument, per client), and personal authentication and encryption techniques to ensure the authenticity of the payer and transaction information integrity. Additional controls include the use of certified tamper-resistant equipment (e.g., EFT/POS terminals), logical access controls to verify transactions, on-line verification of account balances, logging of all transactions and attempts to make a transaction, and the use of serial numbers and check digits.

Procedural measures include 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. 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 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 associations require vendors to match the cardholder's signature on the card with the signature on the payment voucher at the point of sale. The associations have also introduced extensive monitoring and reporting controls to limit fraudulent bankcard activity.

AUDIT

Action Summary

Due to the potential large retail transaction volumes and associated dollar value when initiating payments, internal audit coverage is critical for effective oversight of the financial institution's retail payment systems.

The board of directors should ensure an information technology audit program is in place and designed to test retail payment system internal controls and management policies and procedures. IT audit coverage should include the design and implementation of retail payment products and include the supporting information technology environment encompassing internal data centers, contingency sites, and network infrastructure. IT audit coverage should also verify the adequacy of internal controls in business lines responsible for managing day-to-day retail payment system services.

An effective audit function should include internal and external audit coverage tailored to the complexity of the institution. Due to the potentially large retail transaction volumes

and associated dollar value when initiating payments, internal audit coverage is critical for effective oversight of the financial institution's retail payment systems. The audit coverage should be sufficient to validate the internal control environment surrounding the processing, clearance, and settlement of retail payment transactions. 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 the evaluation they should develop an appropriate schedule of audits. Auditors should review accounting controls and assess the effectiveness of transaction processing, clearance, and settlement processing procedures.

The board of directors should ensure the information technology 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 include the supporting information technology environment encompassing internal data centers, contingency sites, and network infrastructure. IT audit coverage should also verify the adequacy of internal controls in applicable business lines responsible for managing day-to-day retail payment system services. In addition, internal audit should assess the comprehensiveness of the institution's vendor management program and ensure the institution is appropriately managing vendor risk.[20]

INFORMATION SECURITY

Action Summary

Financial institutions must 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. Physical controls should limit access to only those staff assigned responsibility for supporting the operations and business line centers processing 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 appropriately identifying and authenticating retail payment system customers to help ensure retail payment systems integrity.

Financial institutions must implement the appropriate physical and logical security controls to ensure retail payment system transactions are processed, cleared, and settled

[20] See *IT Handbook* "Audit Booklet."

in an accurate, timely, and reliable manner. Retail payment systems contain confidential customer information subject to GLBA section 501(b) security guidelines. 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. Those risk assessments should consider physical and logical security controls for the origination, approval, transmission, and storage of retail payment systems transactions.

Physical controls should limit access to those staff assigned responsibility for supporting the operations and business line centers processing retail payment and accounting transactions. Physical controls should also provide for the ability to monitor and document access to these facilities.

Institution management should assign appropriate logical access controls 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 if the institution has not implemented more robust authentication techniques.

Logical access controls should restrict access on a need-to-know basis and assign access to retail payment applications and data based on functional job duties and requirements. Logical access control should also protect network access. An institution's risk assessment should require it to protect retail payment systems from unauthorized access through appropriate network configuration, firewalls, or intrusion detection. The assessment should review the security of all third-party service providers as well. 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 appropriately identifying and authenticating 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 personal identification numbers (PIN). These controls should minimize bankcard processing errors and fraud and protect the confidentiality of customer and institution information.

The use of newer technologies, including smart cards, wireless phones, and the Internet, presents new security challenges. It is increasingly difficult to implement effective identification and authentication techniques as well as verifying the integrity of the transaction data while preventing customer repudiation.

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 virtual private networking [VPN]). The institution should establish a secure session from the time a consumer enters their personal banking information to 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. To discourage fraudulent transactions, management should consider implementing multi-factor authentication techniques for sensitive retail payment applications. Using digital certificates, leveraging the PKI (public key infrastructure), and employing biometrics, and card or token-based techniques can provide cost-effective solutions for augmenting traditional technical controls.[21]

BUSINESS CONTINUITY PLANNING

Action Summary

Financial institutions should evaluate the extent to which retail payment system products and services provide mission-critical services. Management should perform business impact analyses, and develop business continuity plans accordingly. Management should also conduct an appropriate level of testing to ensure the institution meets customer and counter-party expectations and requirements. Vendor management programs should include provisions for the restoration of service at service providers in the event of a disruption and evaluate service provider business continuity test plans.

Effective business continuity planning is an important component in managing operational risk. Financial institutions and technology service providers 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. [22]

For financial institutions offering basic retail payment products and services (e.g., bankcard issuance, check item processing, branch ATM access, and Internet banking services), business continuity plans should include appropriate recovery targets for each

[21] See *IT Handbook* "Information Security Booklet" and the FFIEC authentication guidelines "Authentication in an Electronic Banking Environment", August 8, 2001.

[22] See *IT Handbook* "Business Continuity Planning Booklet."

retail product. The recovery targets should consider the reliance on any third-party vendors 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 time frames that are reasonable for internal business units as well as other dependent financial institutions and counter-parties. 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 counter-parties to ensure plans are sufficient.

VENDOR AND THIRD-PARTY MANAGEMENT

Action Summary

Financial institutions must establish and maintain effective vendor and third-party management programs.

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 turn key systems. However, institutions contract many retail payment-related services to third parties 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 appropriate contract provisions and adequate due diligence processes. They should also monitor service providers for compliance. 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 as well as electronic bankcard, debit card, and ACH transactions. The financial institution must also maintain effective control over service provider access to customer and financial institution information consistent with GLBA

501(b). Contractual provisions should define the terms of acceptable access and potential liabilities in the event of fraud or processing errors.[23]

OPERATIONS

Action Summary

Financial institutions should develop and implement effective operational risk management programs to mitigate the risks of providing retail payment system services and products.

Financial institutions should adopt measures that limit operational risks for the processing, clearing, and settlement of retail payments. Financial institutions and 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, organizations should adopt business continuity plans to provide solutions and to manage interruptions. Risk analysis should identify confidential assets, critical operations, and potential threats. It should also define safeguards and countermeasures to provide appropriate protection.

Institutions can control fraud risk by using fraud databases and fraud analysis tools. Some bankcard associations and Internet-banking applications use neural network technologies or behavioral fraud analysis. They represent specialized software and hardware designed to identify patterns of behavior, allowing financial institutions to identify suspicious transactions or spending. The bankcard associations 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 institutions and service providers to develop additional databases to provide early identification of potential fraud.

Institutions can also mitigate operational risk by identifying and evaluating potential legal and compliance risks. They can effectively manage operational risk by establishing the appropriate legal review process for the products and services offered. The review process should ensure there are defined roles and responsibilities for retail payment services, specifically for the financial institution and its customers. Reliance on third parties for retail payment products and services should also require a thorough legal review process that supports an effective vendor management program. Institutions should also enforce the regulations and consumer compliance mandates that apply to retail payment services (e.g., Regulation E).

[23] See FFIEC outsourcing guidelines, "Risk Management of Outsourced Technology Services", November 28, 2000, and the *IT Handbook*, "Outsourcing Technology Services Booklet."

RETAIL PAYMENT INSTRUMENT SPECIFIC RISK MANAGEMENT CONTROLS

Action Summary

Specific retail payment instruments introduce risks that require effective internal controls, and adherence to clearinghouse, association, interchange, and regulatory requirements. In addition, financial institutions should develop comprehensive information security and business continuity planning programs that effectively provide for the integrity, confidentiality, and availability of retail payment system products and services.

CHECKS

Return items are a major risk facing institutions that collect checks. A check will be returned to the depositary financial institution if the paying financial institution determines not to pay it (return item). Reasons for returned items include insufficient funds in the account, a closed account, a stop payment order, a fraudulent signature, or failure of the paying financial institution.

The Expedited Funds Availability Act (Regulation CC) obligates institutions to make funds available for customer withdrawal in accordance with mandatory schedules. Thus, a depositary financial institution may be required to make funds available to the customer before an unpaid check is returned to the depositary financial institution. When the depositary institution receives a return item, it will charge back its depositing customer's account for the item even if it has already made the funds available to the depositing customer.

The depositary is exposed to credit risk if the customer does not have sufficient funds in his or her account to cover the returned check. When a paying financial institution returns the item to the depositary, the paying institution does not have to return the item through the same clearing mechanism from which it received the item.

One compensating control for check return items is credit monitoring. Financial institutions should perform a credit assessment of those customers for which they collect large dollar volumes of checks. Financial institutions should also monitor the payment activity of their customers and take appropriate action when credit limits are exceeded. 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 depositary financial institution in case the customer tries to withdraw funds represented by the "bad" check.

Using electronic check presentment (ECP) for payment may reduce risk to depositary financial institutions because it permits them to deliver check data to paying financial

institutions more quickly than with checks. The shorter delivery time permits paying financial institutions to (1) identify checks that cannot be paid and (2) notify the depositary financial institution about those returned checks using an electronic return notice, up to one day earlier than would occur with the physical exchange of paper checks.

However, check truncation —the conversion of MICR information to electronic form— introduces the risk of unauthorized changes to converted check information in transmission or in storage. 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 ensuring the MICR and check image databases are protected from unauthorized access.

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 institution on all checks the business has issued. The financial institution then compares this information with 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.

CREDIT CARDS

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

Consumer compliance regulations and association operating rules provide significant consumer protection for fraudulent transactions. For example, if cardholders timely report the loss of their credit cards, they are responsible, at most, for $50 of the charges resulting from fraud. The issuing financial institution or the merchant pays the costs of any fraud involving credit cards. The merchant should minimally 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 to cover the fraudulent transaction through the chargeback process if it does not follow the minimum procedures.

This has become a significant issue for many on-line retailers processing card-not-present transactions. The major bankcard associations, however, are introducing services to reduce the liability of merchants. Under one initiative, issuers will assume losses for fraudulent transactions if the payment was authorized using the bankcard association's authentication technique.

One control method financial institutions use to reduce risk is the authorization process (approval of 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 (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, institutions can more effectively control credit losses.

DEBIT/ATM CARDS

For debit or ATM cards, there is the risk that unauthorized individuals will obtain them and make fraudulent transactions. There is also a risk to customers' physical safety at ATM locations. Financial institutions and 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 statutes protect consumers by limiting their liability if they give notice of lost, stolen, or mutilated cards within a specified period.

ATM stand-in arrangements, while enabling 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.

The embossing and encoding of blank plastic card stock, if done in-house, should be performed in a secure area and include blank card stock 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 of card stock and accounting should exist for all cards not under dual control. Adequate controls should also exist for captured cards.

Accountability controls should also be established to ensure all cards initially disbursed from the storage area are 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 validated within a few days to ensure that no theft has taken place.

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

The PIN should not appear in printed form, and staff members should not be able to retrieve or display a customer PIN on-line. 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 when 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 PIN is forgotten, the customer should select a new one rather than having staff retrieve the old one.

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

MERCHANT ACQUIRING

For merchant processors, significant operational (transaction) and credit risks require careful monitoring. Chargebacks can create significant credit risk to merchant processors if their merchants cannot honor chargebacks from cardholder disputes. When the merchant is unable to pay its chargebacks due to bankruptcy or fraud, the acquiring financial institution must cover the chargeback and pay the issuing bank. Acquiring financial institutions should carefully manage the merchant portfolio and employ

appropriate underwriting, chargeback processing, and fraud monitoring to mitigate the risk.

Operational (transaction) risk is also present in the bankcard clearing process when sales information is transmitted to card-issuing institutions.[24] Operational risk can also arise from improper processing of bankcard transactions, inadequate internal controls, employee error or malfeasance, and other operational challenges.

EFT/POS AND CREDIT CARD NETWORKS

There should be accurate audit trails for all transactions at each network switch point. The audit trails should identify the originating terminal and destination. In order to ensure accurate transaction posting, adequate procedures should be 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 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, there should be 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 as well as assign responsibility for corrective action. Grievance procedures and arbitration policies are also an important part of participant agreements.

ACH

For ACH credit entries, the ODFI incurs credit risk upon initiating the entries until its customer funds the account. The RDFI incurs credit risk if 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

[24] Information is sent to the bankcard associations first, then the issuing financial institutions. The associations specify debit and credit postings.

may suffer a loss if the originator's account has insufficient funds, is closed, or is frozen because of bankruptcy or other legal action.

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. To manage its credit exposures, an ODFI (and its service provider) 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.

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 financial services, including ACH transactions. The notice, authorization, 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 Office of Foreign Assets Control (OFAC) requirements concerning the accounts of 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 other obligations without incurring losses. Financial institutions should consider the volume of their uncollected ACH transactions as part of their liquidity risk management practices.

While a financial institution's responsibilities do not change with the use of a third-party for ACH processing, its risk exposure may increase as a result of third-party direct access to an ACH operator. A third-party service provider may transmit ACH transactions directly to an ACH operator using the ODFI routing number, provided it has obtained permission from the ODFI. 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 third-party service provider operations. The ODFI should maintain control over its settlement accounts.[25]

In addition, NACHA rules require third-party service providers performing ACH processing functions on behalf of an ODFI or RDFI to conduct an annual compliance audit covering the requirements of the NACHA rules. The financial institution should review and assess all audits of its service provider's internal controls.

[25] See Interagency Outsourcing Guidance and *IT Handbook* "Outsourcing Technology Services Booklet."

The NACHA rules require the ODFI to have an agreement with the third-party service provider with direct access to an ACH operator. Although the federal regulators do not enforce the NACHA rules, a financial institution with appropriate risk management will have an agreement. 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/ODFI agreement;
- ODFI dollar limits for files that a third-party service provider deposits with the ACH Operator. The service provider should notify the ODFI of any files exceeding established dollar limits before depositing it at the ACH Operator so that the ODFI can either approve it as an exception or hold it until the next day; and
- A provision that restricts the third-party service provider's ability to initiate corrections to files already transmitted to the ACH Operator. The ODFI should restrict correction capability. If the third party service provider 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.[26]

INTERNET AND TELEPHONE-INITIATED ACH

Financial institutions originating ACH debit entries through the Internet should ensure they are in compliance with NACHA requirements for Internet-initiated ACH entries. The NACHA rules established a WEB standard entry class (SEC) code for Internet-initiated ACH debit entries for 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 standards.

Financial institutions originating telephone-initiated (TEL) ACH debit transactions for consumers purchasing goods and services should comply with the NACHA rules for the TEL SEC. Although the TEL SEC facilitates the use of one-time automated consumer payments, recent evidence suggests that intentional misuse of the TEL SEC through

[26] 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 third-party service provider.

fraudulent telemarketing practices is resulting in an increasing number of unauthorized consumer ACH debit entries.

Financial institutions offering TEL origination services on behalf of their customers should adopt the appropriate NACHA risk management practices and may be exposed to substantial risk if originating payments for merchants engaged in fraudulent or deceptive business practices.

APPENDIX A: EXAMINATION PROCEDURES

EXAMINATION OBJECTIVE: Examiners should use the Retail Payment Systems Examination Procedures to determine the adequacy of the financial institution's and third-party service provider's policies, business processes, personnel, and internal control systems used to mitigate the risks of retail payment systems. Retail payment system services include checks and share draft item processing, bankcards, payment cards, automated clearinghouse (ACH), EFT/POS networks, and electronic bill payment and person-to-person payment systems. An examiner should base the scope of the examination on his or her assessment of the risks and risk management practices relating to the financial institution's retail payment system services. 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.

Financial institutions are exposed to numerous risks in providing retail payment system services to customers. Depending on the complexity of retail payment system activity, the examination coverage may require an integrated team approach that includes the knowledge and skills of safety and soundness examiners, IT examiners, and credit and compliance specialists.

The examination procedures may be part of either an IT or safety and soundness examination. Examiners can use the examination procedures in their entirety or in a modular fashion to focus on particular retail payment system products or business lines. Depending on the size and complexity of the financial institution or service provider, not all of the procedures are necessary to arrive at a conclusion regarding the quality of risk management practices and performance.

- Tier I objectives and procedures evaluate the effectiveness of the financial institution and service provider's retail payment systems internal controls and risk management processes that may be relied upon for the purpose of identifying and managing risks.

- Tier II objectives and procedures provide additional validation as warranted by the risks to verify the effectiveness of the financial institution's and service provider's retail payment systems function.

TIER I OBJECTIVES AND PROCEDURES

Objective 1: Determine the scope and objectives of the examination of the retail payment systems function.

1. Review past reports for comments relating to retail payment systems. Consider:

   - Regulatory reports of examination, including consumer and compliance information.
   - Internal control self-assessment 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 association, interchange, and clearinghouse documentation relating to services provided by the financial institution, particularly the NACHA required annual security audit and bankcard association self assessments.
   - Supervisory strategy documents, including risk assessments.
   - Prior examination work papers.

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

   - Internal controls, including physical and logical access controls in the data entry area, data center, and item processing operations.
   - EFT/POS network controls.
   - 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. Identify and obtain during discussions with financial institution or service provider management:

   - A description of the retail payment system activity performed, including transaction volumes, dollar amounts, and scope of operations, including check item processing, ACH, bankcard issuing and acquiring, clearance, settlement, and EFT/POS network activity.

- 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, and services since the last examination, particularly the introduction of new retail payment systems incorporating electronic bill presentment and payment (EBPP), stored-value cards, or P2P payment systems.

- A listing of all clearinghouse settlement arrangements in which the financial institution participates. Evaluate the methodology used by the financial institution in assessing its 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.

4. Review the financial institution's response to any retail payment systems issues raised at the last examination. Consider:

   - Adequacy and timing of corrective action.

   - Resolution of root causes rather than specific issues.

   - Existence of outstanding issues.

Objective 2: Determine 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:

   - Data center and network management and the quality of internal controls over internal ATM networks and gateway connectivity to regional and national 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 GLBA 501(b) compliance policies relating to retail payment system generated customer data.

- Assess management's ability to manage outsourcing relationships with retail payment system service providers and software vendors in order to evaluate the adequacy of terms and conditions, and ensure each party's liabilities and responsibilities are clearly defined. Consider:

  - 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 association, and interchange).

  - Adequacy of contract provisions for personnel, equipment, and related services.

  - Adequacy of provisions to obtain management information systems (MIS) needed to monitor the third-party's performance appropriately.

- 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 outage.

  - Alternative access mechanisms in the event of an outage to main access to bankcard, ACH, and other retail options.

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

   - Adequacy and quality of staff resources.

   - Effectiveness of policies and procedures outlining department duties, including job descriptions.

Objective 3: Determine the quality of risk management and support for bankcard issuance and acquiring (merchant processing) activity.

1. Evaluate financial institution adherence to bankcard association rules and bylaws and regulatory guidance.

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

6. 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.

7. 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.

8. For financial institutions involved in bankcard acquiring (merchant processing) services, determine the appropriateness of controls over merchant services. Consider the adequacy of:

   - New merchant approval and acceptance process, termination procedures, and underwriting guidelines for merchant accounts.

   - Fraud and credit monitoring procedures for all established merchant accounts.

   - Chargeback processing procedures and controls, including the volume, age, and losses associated with merchant chargebacks.

   - Agent bank programs (for which the financial institution performs merchant processing for other institutions), and the level of liability assumed by the acquiring financial institution.

Objective 4: Determine the quality of risk management and support for EFT/POS processing activity.

1. Evaluate financial institution 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 cardstock 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 service 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 activity 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.

Objective 5: Determine the quality of risk management and support for ACH processing activity.

1. Evaluate financial institution adherence to NACHA and clearinghouse operating rules and regulations.

2. 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. Also determine that payments in excess of established credit limits are properly authorized.

3. Determine if 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 if management monitors drawings against uncollected funds to ensure they are within established guidelines.

4. 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. Consider:

   - Whether contracted third-party service providers, originating customer entries, are also customers of the financial institution.

   - Whether the agreements include recognition of all relevant NACHA requirements.

   - Whether ACH clearinghouses to which the financial institution is a member, stipulate the funding arrangements (outgoing), Expedited Funds Availability Act (Regulation CC), UCC4A (credit transfer only), and Electronic Funds Transfers (Regulation E).

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

6. Determine if management monitors originating customers for unreasonable numbers of unauthorized ACH debits. If high, this could expose the institution to greater loss.

Objective 6: Determine 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, stored-value cards, and P2P 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 vendors 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 internal controls effectiveness and consumer compliance provisions. Consider:

   - Information security, including identification and authentication systems, in the deployment of any smart cards, EBPP, and P2P product offerings.

   - Customer disclosure and compliance information to 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 determine its effectiveness in including these product offerings in its traditional retail payment operations. Consider:

   - The integration of new retail payment product offerings with existing clearance, settlement, and accounting functions.

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

Objective 7: Determine the quality of risk management and support for checks.

1. Determine if the accounting department handles check return item processing appropriately and reconciles all aged items.

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

   - 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. Determine whether the logical access controls over the electronic files sent by commercial businesses are adequately controlled.

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 systems 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 or recommendations in the report of examination.

   - Potential impact of your conclusions on the Uniform Rating System for Information Technology (URSIT) composite and component ratings.

4. Discuss your findings with management and obtain proposed corrective action for significant deficiencies.

5. Document your conclusions in a memo to the EIC that provides 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 OBJECTIVE AND PROCEDURES

Examination Objective: The 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.

Objective 1: EFT/POS and Bankcard Agreements and Contracts

1. If the financial institution is a participant in a shared EFT/POS network or contracts with a third-party bankcard-issuing or -acquiring processing service providers, consider 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 vendors 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 vendor and the institution.

   - Agreements include a provision of minimum acceptable control standards, the ability of the institution to audit the vendors 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 and audit reports.

Objective 2: Personal Identification Numbers (PIN)

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

Objective 3: Information Security

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

   - 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. Consider:

   - Whether management bases controls on separation-of-duties principles routinely implemented for the processing of financial transactions.

   - Whether identification and authentication schemes include requiring unique logon identifiers with strong password requirements.

   - 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.

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 counter-party data. If not encrypted, evaluate the compensating controls to secure retail payment data in transit.

Objective 4: Card Issuance

1. Assess bankcard issuance activities, and review control procedures. Consider if 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 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 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 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 period of time in between the card and PIN mailing.

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

Objective 5: Business Continuity Planning

1. Assess the financial institution's business continuity plans and review the adequacy of these plans for a partial or complete failure of each retail payment system. Determine if 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 time periods.

   - Stand-in arrangements with other financial institutions included within the plan, allowing for interim bankcard processing in the event of an outage.

   - Adequate testing of plans accounting for various recovery scenarios.

Objective 6: 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. Consider whether:

   - Accounting reconciles bankcard and ATM transaction origination 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 nonposted items, rejects, and differences. Management should periodically receive aging reports that list outstanding items.

5. Assess the 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, consider if 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.

Objective 7: EFT/POS Operational Controls

1. Assess the effectiveness of personnel responsible for internal ATM processing. Consider 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. Assess terminal and operator identification codes used for all retail ATM and POS transactions.

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

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

5. Assess retail EFT equipment keyboards or display units to ensure that they are properly shielded to avoid disclosure of customer IDs or PINs.

6. Assess receipt issuance to ensure 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 verification procedures for telephone-instructed payments or transfers and ensure confirmations are promptly sent to customers and merchants.

10. Assess 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.

Objective 8: ACH ODFI and RDFI Responsibilities

1. Determine if 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 if the ODFI has established procedures to monitor the creditworthiness of its originator customers on an ongoing basis. Consider 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 if the ODFI has established ACH exposure limits for originators. Consider 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 service provider.
   - Written agreements with originators address exposure limits.
   - A separate limit for WEB entries and other high-risk ACH transactions, as warranted, have been established.

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

- The ODFI adjust 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 if the ODFI has implemented procedures to monitor ACH entries initiated by an originator relative to its exposure limit across multiple settlement dates. Consider whether:

   - The monitoring system is automated and accumulates entries for a period at least as long as the average ACH debit 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 separately accumulated and monitored, yet integrated into the overall ACH transaction monitoring system.

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

7. Determine the ODFI's practices regarding originators' annual or more frequent security audits of physical, logical, and network security. Consider 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 third-party service providers. Consider whether:

   - The service provider's financial information is obtained and satisfactorily analyzed.

   - Service-level agreements are established and monitored.

9. Determine if the ODFI allows third-party 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 if the RDFI acts promptly on consumers' stop-payment orders.

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

14. Determine if 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 are satisfactory regarding any audit exceptions.

Objective 9: ACH Accounting and Transaction Processing

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

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

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

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

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

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

7. Assess 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 processors 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. Assess 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. Assess 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. Assess the customer profile origination and change request process. Consider whether requests:

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

Objective 10: ACH Funding and Credit

1. Assess the process for releasing payments to an ACH operator, and determine that assurances are obtained that sufficient collected funds (e.g., on deposit or pre-

funded) or credit facilities are available. The institution should monitor customer intraday and interday positions based on defined thresholds.

2. For third-party processors 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 if management blocks funds (held for disposition) or maintains them in separate accounts until the transaction date.

4. For non pre-funded arrangements, the institution should place blocks on outgoing payments to deposit accounts, apply them as reductions to credit lines, or include them in the overall funds transfer monitoring process.

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

8. Assess 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 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 any audit conducted by the ACH service provider, pursuant to the NACHA rule compliance audit requirement.

Objective 11: 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. Consider whether they:

   - Are in writing and are 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. Consider 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. Also determine if 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 if the ODFI requires its originator to employ a commercially reasonable method to authenticate the consumer/business. Consider whether:

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

4. Determine if the ODFI conducts risk assessments of its originators and if the risk assessments 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.

Objective 12: ACH Contingency Plans

1. Evaluate the ACH contingency plan, determine whether the financial institution has tested it, and determine 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 if 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 if data and program files are adequately retained and backed up at off-premises facilities.

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

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

Objective 13: Checks

1. Determine whether the institution manages check return items effectively and whether there are significant numbers of return items.

2. Determine if the institution records source document images for recovery if the originals are lost in transit.

3. Note whether the institution reconciles batch dollar totals after processing.

4. Determine whether reject items are properly segregated from other work.

5. Note whether exception items are adequately controlled and tracked.

6. Determine whether item processing duties are appropriately segregated.

APPENDIX B: GLOSSARY

Account Balancing Monitoring System (ABMS)	The Federal Reserve's computing system providing reserve account information to the Federal Reserve Banks and depository institutions (DI) on an intraday basis. ABMS serves both as an informational source and a monitoring tool. This information includes opening balances, funds and security transfers, accounting activity, and DI cap and collateral limits.
Acquirer fee	Fee paid to the acquirer of the merchant sales draft. The acquirer of the sales draft collects a merchant discount fee (or processing fee) from the merchant for the costs associated with processing the transaction.
Acquiring bank and acquirer	*See Merchant acquirer.*
Address verification service (AVS)	Bankcard association service that verifies the customer provided billing address matches the billing address on their credit card account. The bankcard associations will not support merchants that opt not to use AVS if those transactions are disputed and will charge the merchant an additional 1.25 percent on those sales.
Agent bank	A member of a bankcard association that agrees to participate in an acquirer's merchant processing program. The agent may or may not be liable for losses incurred on its merchant accounts. An agent is usually a small community financial institution that wants to offer merchant processing services as a customer service. Agent banks that only refer merchants to an acquiring financial institution's program are known as referral banks.
Authentication	The process of verifying the identity of an individual user, machine, software component, or any other entity.
Authorization for ACH	A written or oral agreement between the originator and a receiver that allows payments processed through the ACH Network to be deposited in or withdrawn from the receiver's account at a financial institution.
Automated clearing-house (ACH)	An electronic clearing system in which a data processing center handles payment orders that are exchanged among financial institutions, primarily through telecommunications networks. ACH systems process large volumes of individual payments electronically. Typical ACH payments include salaries, consumer and corporate bill payments, interest and dividend payments, and Social Security payments.

Automated clearing house (ACH) operator	A central clearing facility that depository financial institutions use to transmit and receive ACH entries. ACH operators are typically a Federal Reserve Bank or a private-sector organization that operates on behalf of a depository financial institution (DFI).
Automated teller machine (ATM)	An electronic funds transfer (EFT) terminal that allows customers using a PIN-based debit (ATM) card to initiate transactions (e.g., deposits, withdrawals, account balance inquiries).
Bank Identification Number/Interbank Card Association (BIN/ICA)	A series of assigned numbers used to identify the settling financial institution for both acquiring and issuing bankcard transactions.
Bankcard	A general-purpose credit card, issued by a financial institution under agreement with the bankcard associations (Visa and MasterCard), that customers can use to purchase goods and services and to obtain cash against a line of credit established by the bankcard issuer.
Bankcard associations	Visa U.S.A. and MasterCard International Inc. are bankcard associations established as bank service companies. Financial institutions must be members of an association in order to offer their credit card services. The associations have established membership rights and obligations and membership is limited to financial institutions.
Batch processing	The transmission or processing of a group of related payment instructions.
Card issuer	A financial institution that issues general-purpose credit cards carrying one of the two bankcard association logos. The issuing financial institution establishes the credit relationship with the consumer.
Card verification code (CVC2)	Numeric security code printed on the back of MasterCard credit cards. CVC2 reduces credit card fraud and chargeback instances significantly when used in conjunction with AVS. *See Address verification service (AVS)*.
Card verification value (CVV2)	Three-digit security number that is printed on the back of most Visa credit cards. CVV2 reduces credit card fraud and chargeback instances significantly when used in conjunction with AVS. *See Address verification service (AVS)*.

Cash letter	A group of checks accompanied by a paper listing sent to either a clearinghouse, Federal Reserve, or another financial institution. A cash letter contains a number of negotiable items, usually checks, accompanied by a letter listing the amounts and instructions for transmittal to another financial institution (may also be called a transmittal letter). An incoming cash letter is received by a financial institution from a clearinghouse, Federal Reserve, or another financial institution and contains checks written on accounts at the institution that were cashed elsewhere. An outgoing cash letter is sent to a clearinghouse, Federal Reserve, or another financial institution and contains checks deposited at the institution which are written on accounts at other institutions.
Chargeback	A transaction generated when a cardholder disputes a transaction or when the merchant does not follow bankcard association procedures. The issuer and acquirer research the facts to determine which party is responsible for the transaction. The acquirer will have to cover the chargeback if the merchant is unable to pay.
Check	A written order from one party (payer) to another (payee) requiring the payer's financial institution to pay a specified sum on demand to the payee or to a third party specified by the payee.
Check clearing	The movement of a check from the depository institution at which it was deposited back to the institution on which it was written. The funds move in the opposite direction, with a corresponding credit and debit to the involved accounts.
Check truncation	The practice of holding a check at the institution at which it was deposited (or at an intermediary institution) and electronically forwarding the essential information on the check to the institution on which it was written. A truncated check is not returned to the writer.
Clearance	The process of transmitting, reconciling, and in some cases, confirming payment orders or financial instrument transfer instructions prior to settlement.

Clearing corporation	A central processing mechanism whereby members agree to net, clear, and settle transactions involving financial instruments. Clearing corporations fulfill one or all of the following functions: - Nets many trades so that the number and the amount of payments that have to be made are minimized, - Determines money obligations among traders, and - Guarantees that trades will go through by legally assuming the risk of payments not made or securities not delivered. This latter function is what is implied when it is stated that the clearing corporation becomes the "counter-party" to all trades entered into its system. Also known as a clearinghouse or clearinghouse association.
Clearinghouse associations	Voluntary associations, formed by financial institutions that establish an exchange for checks drawn on those institutions. Typically, institutions participating in check clearinghouses use the Federal Reserve's national settlement service for the checks exchanged each business day.
Clearinghouse for Inter-Bank Payment Systems (CHIPS)	A "real time", multilateral final payments system for large dollar value business-to-business payment transactions between domestic or foreign institutions that have offices located in the United States. CHIPS is run by CHIP Co. L.L.C., a subsidiary of the Clearing House.
Commercially reasonable	Hardware and software made available by a reputable firm for use in a commercial environment. Practices and procedures in widespread use in the business community generally considered to represent prudent and reasonable business methods.
Consumer account	A deposit account held by a participating DFI and established by a natural person primarily for personal, family, or household use and not for commercial purposes.
Consumer	Usually refers to an individual engaged in noncommercial transactions.
Correspondent bank	An institution, acting on behalf of other institutions, that can settle the checks they collect for other institutions (respondents) by using accounts on their books or by sending a wire transfer. Generally, a provider of banking and payment services to other financial institutions.

Credit card	A card indicating the holder has been granted a line of credit. It enables the holder to make purchases or withdraw cash up to a prearranged ceiling. The credit granted can be settled in full by the end of a specified period or can be settled in part, with the balance taken as extended credit. Interest is based on the terms of the credit card agreement and the holder is sometimes charged an annual fee.
Credit entry	An entry to the record of an account to represent the transfer or placement of funds into the account.
Daylight overdraft	A daylight overdraft occurs at any point in the business day when the balance in an institution's account becomes negative. Daylight overdrafts can occur in accounts at Federal Reserve Banks as well as at private financial institutions. Daylight credit can also arise in the form of net debit positions of participants in private payment systems. A daylight overdraft occurs at a Federal Reserve Bank when there are insufficient funds in an institution's Federal Reserve Bank account to cover outgoing funds transfers or incoming book-entry securities transfers. An overdraft can also be the result of other payment activity processed by the Federal Reserve Bank, such as check or automated clearinghouse transactions.
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*
Depositary bank	The institution at which a check is first deposited.
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	An institution that accepts deposits.

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 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 (POS) to the processor's database.
Expedited Funds Availability Act (EFAA)	*See Regulation CC.*
Electronic funds transfer (EFT)	A generic term describing any transfer of funds between parties or depository institutions through electronic data systems.
Electronic Funds Transfer Act (EFTA)	The Electronic Funds Transfer Act and Regulation E are designed to ensure adequate disclosure of basic terms, costs, and rights relating to electronic fund transfer (EFT) services provided to consumers. Institutions offering EFT services must disclose to consumers certain information, including: initial and updated EFT terms, transaction information, periodic statements of activity, the consumer's potential liability for unauthorized transfers, and error resolution rights and procedures. EFT services include automated teller machines, telephone bill payment, point-of-sale transfers in retail stores, fund transfers initiated through the Internet, and preauthorized transfers to or from a consumer's account.
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.
Exposure limit	Referring to the settlement of operating services, the maximum amount an ACH originator is allowed to originate. This amount can be based on the originator's credit rating, historical or predicted funding requirements, and the type of obligation.
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.
Independent sales organizations(ISO)	A nonfinancial institution organization that provides a variety of merchant processing functions on behalf of the acquirer. These functions include soliciting new merchant accounts, arranging for terminal purchases or leases, and providing backroom services. An ISO is also referred to as a member service provider (MSP). The acquirer must register all ISO/MSPs with the bankcard associations.
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 bank card transaction. Interchange fees generally flow toward the institution funding the transaction and assuming risk in the process. 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, and 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 1.0 to 3.0 percent 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 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.
MICR-line information	Refers to data characters at the bottom of a check. The magnetic ink character recognition (MICR) line includes the routing number of the payer bank, the amount of the check, the number of the check, and the account number of the customer.

Multi-factor authentication	Strong authentication mechanism relying on more than one type of authentication. A PIN or password alone is representative of single factor authentication. Adding additional authentication mechanisms would result in multi-factor authentication.
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.
National Automated Clearing House Association (NACHA)	The national association that establishes the rules and procedures governing the exchange of automated clearinghouse payments.
National Settlement Service (NSS)	(Also referred to as Deferred net settlement). The Federal Reserve's settlement service. A type of payments system in which financial institutions continually send payment instructions over a period of time with final transfer occurring at the end of the processing cycle. During the period, a record is kept of net debits and credits.
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 Assets Control (OFAC)	The Office of Foreign Assets Control, 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.
Originator	A person that has authorized an ODFI to transmit a credit or debit entry to the deposit account of a receiver with an RDFI, or, if the receiver is also the RDFI, to such receiver.
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 mechanisms, 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.
Person-to-person (P2P) payment	On-line 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 presentment fee is a fee that an institution receiving a check may impose on the institution that presents the check for payment. For checks presented by 8 a.m. local time, however, no presentment fee may be charged.
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. Fedwire® 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.
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.
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	A nine-digit number (eight digits and a check number) that identifies a specific financial institution (also referred to as the ABA number).
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(s).
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	3-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.
Third-party service provider (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 DFI.
Truth in Lending Act (TILA)	Regulation Z (12 CFR 226) promulgated by the Board of Governors of the Federal Reserve System prescribing uniform methods for computing the cost of credit, for disclosing credit terms, and for resolving errors on certain types of credit accounts.
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: LAWS, REGULATIONS, AND GUIDANCE

LAWS

- 12 USC 1861-1867(c): Bank Services Company Act
- 12 USC 4001: Expedited Funds Availability Act
- 12 USC 5001: Check Clearing for the 21st Century Act
- 15 USC 1693: Electronic Funds Transfer Act
- 15 USC 6801 and 6805(b): Gramm-Leach-Bliley Act
- 18 USC 1: USA Patriot Act (Pub. L. No. 107-56)
- 31 USC 5311: Bank Secrecy Act

FEDERAL RESERVE BOARD

REGULATIONS

- 12 CFR 210, Subparts A and B (Regulation J): Collection of Checks and Other Items by Federal Reserve Banks and Funds Transfers through Fedwire
- 12 CFR 205 (Regulation E): Electronic Fund Transfers
- 12 CFR 229, Subparts A, B, and C (Regulation CC): Availability of Funds and Collection of Checks

GUIDANCE

- Board of Governors of the Federal Reserve System Payments System Risk (PSR) Policy, December 2001
- Federal Reserve Operating Circular No. 4, May 18, 2003
- SR Letter 03–17: New Bank Secrecy Act Examination Procedures Relating to the USA PATRIOT Act, October 2003
- SR Letter 02–18: Section 312 of the USA Patriot Act—Due Diligence for Correspondent and Private Banking Accounts, July 2003
- SR Letter 01–20: FFIEC Guidance on Authentication, August 2001

- SR Letter 01–15: Safeguarding Customer Information, May 2001
- SR Letter 01–11:Identity Theft and Pretext Calling, April 2001
- SR Letter 00–17: FFIEC Guidance on the Risk Management of Outsourced Technology Services, November 2000
- SR Letter 00–04: Outsourcing of Information and Transaction Processing, February 2000
- SR Letter 93–64: Credit Card-related Merchant Activities, November 1993
- SR Letter 03–12: Revisions to the Suspicious Activity Report, May 2003
- SR Letter 97–28: Reporting of Computer Related Crimes by Financial Institutions, November 1997

FEDERAL DEPOSIT INSURANCE CORPORATION

REGULATIONS

GUIDANCE

- FIL 63-2003: Guidance on Identity Theft Programs, August 12, 2003
- 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

REGULATIONS

- 12 CFR Part 721: Federal Credit Union Incidental Powers Activities
- 12 CFR Part 748: Security Program, Report of Crime and Catastrophic Act, Bank Secrecy Act Compliance, and Appendix A – Guidelines for Safeguarding Member Information
- 12 CFR Part 716: Privacy of Consumer Financial Information
- 12 CFR Part 741: Requirements for Insurance
- 12 CFR Part 740: Advertising

GUIDANCE

- NCUA Letter to Credit Unions 01–CU–20: Due Diligence Over Third–Party Service Providers, November 2001
- NCUA Letter to Credit Unions 01–CU–09: Identity Theft and Pretext Calling, September 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 01–CU–11: Electronic Data Security Overview, August 2001
- NCUA Letter to Credit Unions 01–CU–10: Authentication in an Electronic Banking Environment, August 2001
- NCUA Regulatory Alert 01–RA–03: Electronic Signatures in Global and National Commerce Act (E-Sign Act,) March 2001
- NCUA Letter to Credit Unions 01–CU–02: Privacy of Consumer Financial Information, February 2001
- NCUA Letter to Credit Unions 00–CU–11: Risk Management of Outsourced Technology Services (with Enclosure,) December 2000
- NCUA Letter to Credit Unions 00–CU–02: Identity Theft Prevention, May 2000
- NCUA Regulatory Alert 99–RA–3: Pretext Phone Calling by Account Information Brokers, February 1999

OFFICE OF THE COMPTROLLER OF THE CURRENCY

REGULATIONS

GUIDANCE

- Office of the Comptroller of the Currency (OCC) Comptroller's Handbook: Credit Card Lending, October 1996
- OCC *Comptroller's Handbook*: Merchant Processing, December, 2001
- OCC Advisory Letter 96–7: Credit Card Pre-Approved Solicitations, September 1996
- OCC Advisory Letter 2000–6: Audit and Internal Controls, July 2000
- OCC Advisory Letter 2000–9: Third-Party Risk, August 2000
- OCC Advisory Letter 2000–10: Payday Lending, November 2000

- OCC Advisory Letter 2000–12: Management of Outsourcing Technology Services, November 2000
- OCC Bulletin 97–24: Credit Scoring Models, Examiner Guidance, May 1997
- OCC Bulletin 99–10: Interagency Guidance on Subprime Lending, March 1999
- OCC Bulletin 99–15: Subprime Lending: Risks and Rewards, April 1999
- OCC Bulletin 2000-3: FFIEC Consumer Credit Reporting Practices, February 2000
- OCC Bulletin 2000–16: Risk Modeling, Model Validation, May 2000
- OCC Bulletin 2000–20: FFIEC Uniform Retail Credit Classification and Account Management Policy, June 2000
- OCC Bulletin 2001–6: Expanded Guidance for Subprime Lending Programs, January 2001
- OCC Bulletin 2001–47: Third Party Relationships, Risk Management Principles, November 2001
- OCC Bulletin 2002–2: ACH Transactions Involving the Internet, January 2002
- OCC Bulletin 2003–01: Account Management and Loss Allowance Guidance, January 2003

OFFICE OF THRIFT SUPERVISION

REGULATIONS

- 12 CFR Part 570, Appendix A: Interagency Guidelines Establishing Standards for Safety and Soundness
- 12 CFR Part 570, Appendix B: Interagency Guidelines Establishing Standards for Safeguarding Customer Information

GUIDANCE

- Thrift Bulletin 82: Third Party Arrangements, March 2003
- CEO Letter 84: Electronic Finds Transfers, June 1998
- CEO Letter 113: Internal Controls, July 1999
- Thrift Activities Handbook: Section 340, Internal Control

- Thrift Activities Handbook: Section 341, Technology Risk Controls
- Thrift Activities Handbook: Section 580, Payment Systems Risk