Comptroller's Handbook O-MP

Safety and Soundness

Capital Adequacy (C) | Asset Quality (A) | Management (M) | Earnings (E) | Liquidity (L) | Sensitivity to Market Risk (S) | Other Activities (O)

Merchant Processing

August 2014

Office of the Comptroller of the Currency

Washington, DC 20219

Contents

Introduction **1**
Background 1
Types of Merchant Processors and Other Participants 2
Technological Changes 5
Operations 7
Risks Associated With Merchant Processing 13
Strategic Risk 13
Credit Risk 14
Operational Risk 15
Compliance Risk 16
Reputation Risk 18
Risk Management and Controls 18
Board and Management Supervision 18
Capital Allocation and Limits 19
Security Pledges 21
Payment Card Industry Security Standards Council 21
Merchant Underwriting and Review 22
Pricing 31
Scorecards and Models 33
Managing Third-Party Organizations 34

Examination Procedures **38**
Scope 38
Acquiring Banks 41
Agent Banks 54
Conclusions 58
Internal Control Questionnaire 60
Verification Procedures 69

Appendixes **70**
Appendix A: Portfolio Profile Worksheet 70
Appendix B: Request Letter 73
Appendix C: Profit and Loss Statement 77
Appendix D: Merchant File Review Worksheet 78
Appendix E: Merchant Activity and Capital Worksheet 79
Appendix F: Glossary 80

References **86**

Introduction

The Office of the Comptroller of the Currency's (OCC) *Comptroller's Handbook* booklet, "Merchant Processing," provides guidance for bank examiners and bankers on merchant processing activities. For purposes of this booklet, a merchant processing activity is the settlement of credit and debit card payment transactions by banks for merchants through various card associations. This booklet focuses on card payment-related processing, which is separate and distinct from a bank's business of issuing payment cards. The appendixes provide sample worksheets and a glossary of merchant processing terms. Throughout this booklet, national banks and federal savings associations (FSA) are referred to collectively as banks, except when it is necessary to distinguish between the two.

Background

The principles addressed in this booklet may apply to other types of electronic payments. Processors may cover all types of payment cards or specialize in one form.

A bank's merchant processing activities involve gathering sales information from the merchant, obtaining authorization for the transaction, collecting funds from the card-issuing bank, and reimbursing the merchant. The processing of sales transactions for merchants by the bank does not directly affect the bank's balance sheet except through settlement accounts and reserve balances. Merchant processing can, however, create significant off-balance-sheet contingent liabilities that may result in losses to the bank. Merchant processing is a business of high volumes and low profit margins. Generally, a high level of sales and transaction volume is needed to create a profitable operation in light of the low income generated per transaction. Processing a high transaction volume carries risk; only efficiently run departments can successfully maintain the necessary cost controls and effectively manage the accompanying strategic, operational, compliance, reputational, and credit risks.

As a high-volume business, merchant processing is dominated by a relatively few large and midsize banks, which often use the services of independent sales organizations or membership service providers (ISO/MSP), join partnerships or alliances, or enlist agent banks. The merchant processing business of these banks is intensely competitive, with aggressive pricing.

Bankers need to fully understand merchant processing and its risks. Attracted to the business by the potential for increased fee income, they may underestimate the risks and not employ personnel with sufficient knowledge and expertise. They also may not devote sufficient resources to oversight or perform proper due diligence reviews of third-party organizations. Bankers may not have the managerial experience, resources, or infrastructure to engage safely in merchant processing for merchants with which the bank does not already have a customer relationship or which are located outside the bank's local market area, or to manage high sales volume, high-risk merchants, or high charge-back levels.

There are various types of organizations that make up the electronic payment transaction industry. MasterCard and Visa, which are bank card associations, are the most significant organizations in this industry in terms of number of cards issued and the number of banks issuing its cards. (The OCC does not endorse particular products or brands.) Only financial institutions can become members of one of the bank card associations. MasterCard and Visa are operationally similar, with both using four-party networks to process transactions. The four parties involved in the network are the card issuers (financial institutions that are members of the association), the acquirers, the cardholders, and the merchants. The associations are not counted as a separate group because they are considered the umbrella organizations, and service providers are not counted as a separate group because their function is often served by acquirers.

In addition to the bank card associations, other card companies issue their own cards, authorize purchases, and settle with both consumers and merchants. These card companies use three-party networks to process transactions, instead of a four-party network. A major distinction in the three-party network is that the card issuer and the merchant acquirer are the same entity. Examples of these other card companies include American Express, Discover Card, and Diners Club.

Much of the information in this booklet focuses on the bank card association model and operations.

Types of Merchant Processors and Other Participants

The role and accompanying risks of banks and third-party organizations vary. The most common participants in merchant processing are acquiring banks, agent banks with and without liability, and third-party organizations.

Acquiring Banks

A bank that contracts with merchants for the settlement of card transactions is an acquiring bank. Acquiring banks contract directly with merchants, or indirectly through agent banks or other third-party organizations, to process card transactions. Bank management should be familiar with the potential liability for acquiring banks through this activity.

The acquiring bank generally provides all backroom operations to the agent bank and owns the bank identification number (BIN)/Interbank Card Association (ICA) number through which settlement takes place. A BIN/ICA number is an individual member's unique identification number that facilitates clearing and settlement through the card association. The BIN is assigned by Visa and the ICA number is assigned by MasterCard. Depending on the contractual arrangement with the acquirer, the agent bank may be liable in the event of charge-back or fraud losses.

An acquiring bank that is a member of a card association must sponsor a merchant that accepts sales payments from card association-branded payment cards. The merchant may

then maintain a settlement account with the acquiring bank or settle via automated clearing house (ACH) transactions between the acquiring bank and the merchant's bank.

A merchant may open a merchant account at a bank or other financial institution that is a member of the bank card association. The establishment of this merchant account enables the merchant to facilitate the processing of card transactions.

Agent Banks

The agent bank is typically a community bank that does not directly offer merchant processing services. Community banks refrain from contracting with merchants on their own because they lack the management expertise or the necessary infrastructure needed to serve as acquirers.

An agent bank may refer or want to sign merchants that do not meet the acquiring bank's underwriting guidelines. The acquirer may accept the account on the condition that the agent bank signs an agreement indemnifying the acquirer against losses. When a referral bank indemnifies the acquirer for losses, the referral bank becomes an agent bank with liability for those merchants indemnified. An indemnification agreement is typically used when the agent bank has other account relationships with the merchant and, as a customer service, wants to assist the merchant in obtaining processing services.

Bank managers and examiners should be familiar with the limits on a national bank's ability to indemnify a transaction, as outlined in 12 CFR 7.1017, "National Bank as Guarantor or Surety on Indemnity Bond." Limits on an FSA's ability to enter a repayable suretyship agreement or guaranty agreement are described in 12 CFR 160.60, "Suretyship and Guaranty."

Many community banks have referral arrangements with acquirers; these arrangements are also referred to as agent banks without liability. In referral arrangements, the community banks do not have liability exposure, because they do not indemnify the acquirers for losses. In a typical referral arrangement, the acquirer performs the underwriting, executes the merchant agreement, and accepts responsibility for merchant losses. The acquiring bank may pay the referring bank a fee for brokering the merchant relationship.

Third-Party Organizations

A third-party organization is any outside company the acquiring bank contracts with to provide merchant processing services. Examples of third-party organizations may include ISOs/MSPs, although others exist. The ISO/MSP solicits merchants and performs such services for acquirers as processing merchant applications and charge-backs, detecting fraud, servicing merchant customers, providing accounting services, selling or leasing electronic terminals to merchants, processing transactions, authorizing purchases, and capturing data.

To control costs, acquiring banks frequently outsource functions to third-party organizations. An acquirer's sales and transaction volume may not justify the cost of in-house data

processing, or the bank may not want to staff a direct sales force. Acquirers can benefit from the technological expertise and capabilities of third parties without having to develop the systems and infrastructure themselves. A third-party organization provides a wide array of services. Each acquirer should maintain up-to-date records including a list of third-party organizations used and services outsourced to the third party. Other records that a bank should maintain include contracts, amendments, fee schedules, authorized signatories, and contacts.

The acquiring bank may receive third-party services indirectly. For example, an ISO/MSP may contract directly with a data processor or network provider, and the ISO/MSP may pass the service on to the bank. Banks can also receive services indirectly through an ISO/MSP that contracts with another ISO/MSP to provide services.

There are hundreds of third-party organizations providing services, and the quality of these services can vary widely. Banks should exercise strong due diligence and maintain strong vendor management programs for third-party organizations. For more information, refer to the "Managing Third-Party Organizations" section of this booklet and OCC Bulletin 2013-29, "Third-Party Relationships: Risk Management Guidance." The guidance applies to all banks with third-party relationships.

Bank Card Association Requirements

Because third-party organizations are not bank card association members, acquirers must register third-party organizations with the bank card association before accepting their services. The acquirer must pay an initial registration fee and annual fees to the bank card association for each third party under contract. Typically, this fee is passed on to the third-party organization.

After registration, the acquirer remains responsible for complying with the bank card association's operating rules on business relationships with third-party organizations. These rules make the acquiring bank liable to the bank card association for the actions of the acquiring bank's third parties. The bank card association also requires the acquiring bank to regularly submit information about the acquiring bank's third-party organizations. Acquiring banks can be fined by the bank card association for failing to provide the information. Rules are established by the bank card association and are specific to the individual bank card association.

Special Third-Party Organizations

Payment Facilitator or Payment Service Provider

MasterCard defines a payment facilitator as a merchant that is registered by an acquirer to facilitate transactions on behalf of sub-merchants. Under Visa's rules, a payment service provider is an organization that contracts with an acquirer to provide payment services to sponsored merchants. The payment facilitator and the payment service provider (collectively, PSP) are operationally similar. In both cases, the acquirer is responsible for the actions of its

PSP and the PSP's sponsored merchants. Bank card association rules are specific to the individual association. Banks engaged in merchant processing activities should be aware of specific rules as they relate to payment facilitators and payment service providers.

Rent-a-BIN

Rent-a-BIN,[1] in the acquiring context, describes an arrangement in which an acquiring bank permits the ISO/MSP to use the bank's Visa BIN or MasterCard ICA number to settle merchant card transactions. The bank has minimal operational involvement. The ISO/MSP retains the majority of income, and the bank receives a fee for the use of the BIN/ICA number.

The acquiring bank that owns the BIN/ICA number always retains risk of loss, as well as responsibility for settlement with the bank card association. The bank is responsible based on the contractual provisions of the association membership. Therefore, the bank's management should rigorously oversee and control the Rent-a-BIN arrangement to ensure that the ISO/MSP is appropriately managing the risk. Oversight controls are important, even if the ISO/MSP shares in the liability. Moreover, the acquiring bank must consider any lending relationship the bank has with the ISO/MSP when analyzing the bank's total risk exposure.

For more information on third-party organizations and ISO/MSP relationships, refer to the "Risks Associated With Merchant Processing" and "Risk Management and Controls" sections of this booklet.

Technological Changes

Traditionally, most merchant processing transactions originated from retail credit card purchases. With technological changes, however, debit card purchases, reloadable cards, and other prepaid payment products, as well as electronic benefits transfer (EBT) transactions, are increasing sources of processing volume.

Bank card associations have aggressively promoted the move to electronic transactions through their interchange rate structure. Because of the promoted use by the bank card associations and advances in technology, the majority of payment card sales transactions are now electronic. Paper-based transactions still exist, but to a much lesser degree than electronic transactions.

Technological changes include the expansion of mobile purchases through the use of smartphones. Although mobile transactions have not been a significant source of losses to date, merchant processors are likely to face increased risk exposure in the future from such transactions. Cyber attacks can reduce the availability of online and mobile banking services and, more significantly, result in identity theft and fraud. To date, the volume of mobile payments processed in the United States (that do not use established card or ACH networks

[1] There are also payment card (issuing) Rent-a-BIN relationships with similar requirements for strong vendor management and oversight programs; the issuing Rent-a-BIN has its own set of unique risks and operations, however, which are outside the scope of this booklet.

for authorization, clearing, and settlement) is small relative to the potential market. Consequently, major retailers are in discussions with banks, technology companies, and telecommunications providers to establish a common standard for mobile payments and a payment system to support the growth of these transactions.

Wireless Processing

In recent years, as technological costs have declined, merchants have increasingly used wireless terminals for credit and debit card transactions. Wireless processing is one of the easiest and most convenient ways for merchants to accept payment from customers, and is a cost-effective way to process transactions. The payment card is swiped through a wireless terminal and a customer receipt is printed for the transaction.

The benefits of wireless processing include the following:

- Wireless terminals are easy to use anywhere.
- Swiped transactions are faster to produce than keyed transactions. A swiped transaction can take approximately three to five seconds, while keyed transactions can take one to two minutes.
- The customer's card transaction is approved or declined instantly.

Prepaid Debit Cards

A prepaid debit card that is reloadable is often referred to as a general purpose reloadable card. A consumer can add funds to the card from varying sources, depending on the specific card. Payroll deposits are a frequent source of funds, as are other direct deposits. This is a growing product area for all banks and consumers. Prepaid debit cards include worldwide functionality due to merchant acceptance of the network associated with the card. In addition, more consumers are using the cards as an alternative to credit cards.

Gift Cards

Gift cards are prepaid cards that are generally not reloadable. A cardholder may use a gift card for the purchase of goods or services. A gift card is often used as a noncash monetary gift. The card is identified by a specific number or identification code (card ID), rather than an individual's name, so anyone can use the card. These cards are backed by an online electronic system for authorization. Many cards have no value until they are sold, at which time the cashier enters the amount the customer wishes to put on the card.[2]

Some gift cards can only be used at select retailers, while others can be used anywhere that accepts major payment card brands. If the cards are limited and can only be used at select retailers, they are considered "closed loop" cards. Cards that can be redeemed by various establishments and merchants are considered "open loop" or "network" cards. Some gift

[2] The amount is rarely stored on the card but is noted in the store's database, which is cross-linked with the card ID. Consequently, gift cards are generally not stored-value cards, because a monetary value is not stored on the gift card.

cards may be reloadable, allowing the cardholder to add funds to the card and continue using it. Gift cards have become increasingly popular because they don't require the purchaser, or donor, to select a specific gift. The recipient has discretion in using the gift card within the restrictions set by the issuer.

Operations

This section summarizes how card transactions are processed. The intricacies may vary significantly for each bank, but the basic principles are the same.

Authenticating Transactions

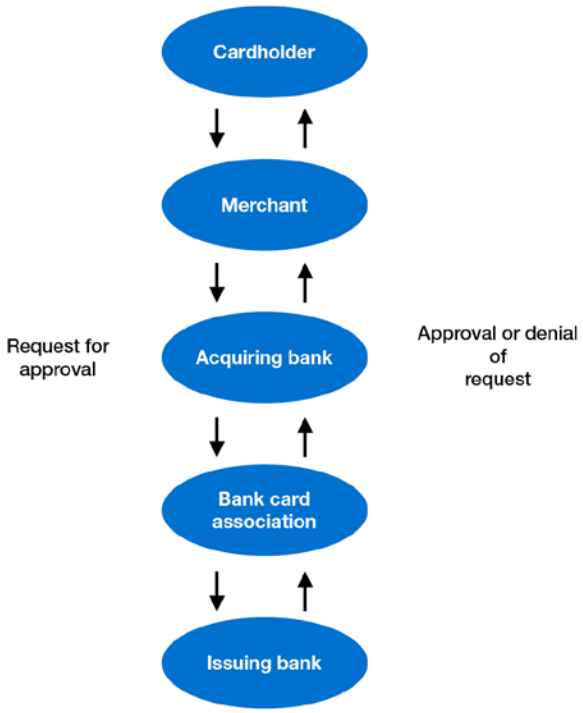
The first step in authorizing payment card transactions is to verify the identity of the individual cardholder. Card association rules address cardholder authentication and vary based on the type of card transaction, the merchant category, the amount of the transaction, and how the cardholder initiates the transaction. This ensures that the person presenting the card for payment is authorized to use the card. Transactions can be authenticated by using a signature code (a three- or four-digit code located typically on the back of the card) or other methods. For details of this process, see the "Information Security" booklet of the Federal Financial Institutions Examination Council (FFIEC) *Information Technology Examination Handbook*.

Europay, MasterCard, and Visa developed EMV (named after the developers), a technology that embeds a microprocessor chip on payment cards to encrypt transaction data. EMV technology is widely used in other countries, but not in the United States. Visa and MasterCard have announced initiatives to encourage U.S. retailers to accept EMV-enabled cards, and acceptance of EMV technology in the United States could alter the authentication process.

Authorizing Transactions

Authorization is the process of approving or declining a transaction before a purchase is finalized or cash is disbursed. After authentication, the merchant obtains approval from the card-issuing bank or from a third party acting on behalf of the card-issuing bank. Figure 1 illustrates the authorization process. This authorization process is structured to prevent transactions from being approved for cardholders who have not satisfactorily maintained their card accounts or who are over their credit limits, and to protect against the unauthorized use of cards that have been reported as stolen or are fraudulent. Authorization systems may include internally or externally developed platforms, or a combination of both.

Figure 1: Authorization Process



Source: OCC

Typically, the clerk or cardholder swipes the card through a terminal at the point of sale to obtain the information stored on the magnetic stripe on the back of the card, and then inputs the amount of the transaction. This information is transmitted to the acquiring bank or the acquiring bank's processor, which captures the transaction and forwards the information to the card-issuing bank through the bank card association network. Depending on the status of the cardholder's account, the transaction is approved or declined, and this decision is transmitted back through the bank card association network to the point of sale.

Bank card associations have implemented simpler rules for some in-person card transactions. For example, customer signatures or personal identification numbers are not required for transactions meeting certain low-dollar criteria and where the merchant's business falls into certain business code categories; authentication, however, is required. The threshold for low-dollar transactions varies depending on the particular bank card association and the approved merchant category code allowed by the bank card association.

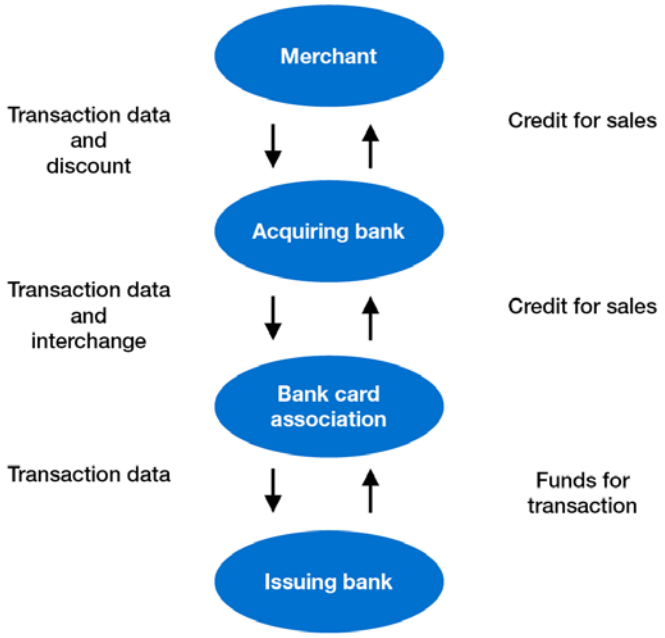
Acquiring banks require authorizations for all paper-based transactions. Ensuring that each paper-based transaction is authorized helps protect merchants against fraudulent transactions. While paper-based transactions still occur, most transactions are now processed electronically.

Clearing and Settlement

Clearing is the process of delivering final transaction data from acquirers to issuers for posting to the cardholder's account. Clearing also includes the calculation of certain fees and charges that apply to the issuer and acquirer involved in the transaction, as well as the conversion of transaction amounts to the appropriate settlement currencies.

Settlement is the process of transmitting sales information to the card-issuing bank for collection and reimbursement of funds to the merchant. Settlement also refers to the process of calculating, determining, and reporting the net financial position of issuers and acquirers for all transactions that are cleared. Figure 2 illustrates the clearing and settlement process. A typical transaction flows from the merchant to the acquirer (or acquirer's processor), then to the bank card association, and finally to the card-issuing bank (or its processor), which bills the cardholder. Funds flow in the opposite direction, or from the card-issuing bank to the bank card association, then to the acquirer, and finally to the merchant. An acquiring bank's outsourcing of some (and sometimes all) of its merchant processing to third-party organizations complicates transaction flows and fund flows.

Figure 2: Clearing and Settlement Process



Source: OCC

Note: The timing of the discount and interchange fees may not directly correspond to the transfer of transaction data as shown in this simplified figure (i.e., the discount fee is typically collected monthly and the interchange fee is collected daily at net settlement). This figure also does not illustrate the added complexities associated with using third-party organizations.

Large merchants often transmit data directly to the acquirer or third-party organization. Smaller merchants usually submit data to a third-party organization that collects data from several merchants. The third-party organization then transmits transactions to the acquirers.

The acquiring bank transmits the information through an interchange to the issuing bank. The issuer remits funds, through the bank card association, to the acquirer and posts the charges to the cardholders' accounts. After the acquirer receives the proceeds, it pays the individual merchants. Most third-party processors net settle with their clients. That is, the bank receives, or pays, the net of merchant and cardholder activity for each day of business.

The acquiring bank may pay select merchants before receiving funds through interchange, thereby increasing the bank's credit and liquidity exposure. The timing of the payments to the merchants is specified in the agreement between the acquiring bank and the merchants. The agreement should always allow the bank to review the transaction for fraud before releasing funds. The acquiring bank should not become reliant on the merchant's deposits to fund other bank activities. An acquiring bank is potentially liable for losses caused by merchant fraud, including merchants engaged in deceptive or misleading practices. A merchant can also directly defraud banks by such means as factoring and laundering. Factoring, also called credit card factoring, is used to launder money via credit cards, essentially by processing transactions through a merchant account for a business or entity other than the specific business that was screened and set up for the merchant account.

Fedwire

The card-issuing bank pays the bank card association using Fedwire, a real-time funds transfer system. A bank must hold an account at a Federal Reserve Bank to use Fedwire, because settlement funds must come from a Federal Reserve account. The card-issuing bank makes the payment by sending a message over Fedwire authorizing the Federal Reserve Bank to electronically debit its account for the net settlement amount and to transfer the funds to the bank card association's settlement bank. These transfers are essentially instantaneous. The bank card association's settlement bank then pays the acquiring bank using Fedwire.

Automated Clearing House

The ACH is an electronic network for financial transactions in the United States that processes large volumes of transactions in batches. Acquiring banks usually pay merchants by initiating ACH credits to merchants' deposit accounts at the merchants' local banks. If an acquiring bank employs a third-party processor, the processor usually prepares the ACH file that facilitates payment. Management should have controls to ensure that the ACH transactions are accurate. Bank employees should follow formal procedures when delaying settlement of a merchant's funds. Such a delay usually occurs because fraud prevention staff at the bank finds a transaction suspicious or unusual. Placing a hold on funds affects the origination of the ACH file. For more information, see the *National Automated Clearing House Association (NACHA) Operating Rules & Guidelines*.

Charge-Back Processing

Charge-backs are common in the merchant processing business, and a merchant must be capable of paying them. Charge-backs fall into four categories.

Technical: Expired authorization, nonsufficient funds, or bank processing error.

Clerical: Duplicate billing, incorrect amount billed, or refund never issued.

Quality: Consumer claims to have never received the goods as promised at the time of purchase.

Fraud: Consumer claims not to have authorized the purchase, or identity theft.

The consumer's rights and responsibilities vary by the type of payment method used. For a credit card, the consumer must first try resolving a payment dispute with the merchant. If unsuccessful, the consumer informs the card-issuing bank of the dispute, and then the card-issuing bank posts a temporary credit to the cardholder's account. The card-issuing bank requests documentation from the merchant that authenticates the transaction and possibly resolves the dispute. If the charge-back is upheld by the card-issuing bank, the amount is charged back to the merchant's account, and the consumer does not pay for the disputed charge. The customer has 60 days[3] from the day the card statement is received to report a dispute to the card-issuing bank.

For debit cards used at a point-of-sale terminal or with other electronic devices, the bank must follow the error resolution process detailed in 12 CFR 1005. This process gives the consumer rights and responsibilities, including:

- Consumer may be liable for an unauthorized electronic fund transfer (EFT) depending on when the consumer notifies the financial institution and whether an access device was used to conduct the transaction. Under the Electronic Fund Transfer Act (EFTA), there is no bright-line time limit within which consumers must report unauthorized EFTs.
- Consumer is generally reimbursed the amount of the error within 10 business days of notification to the bank of the alleged error.

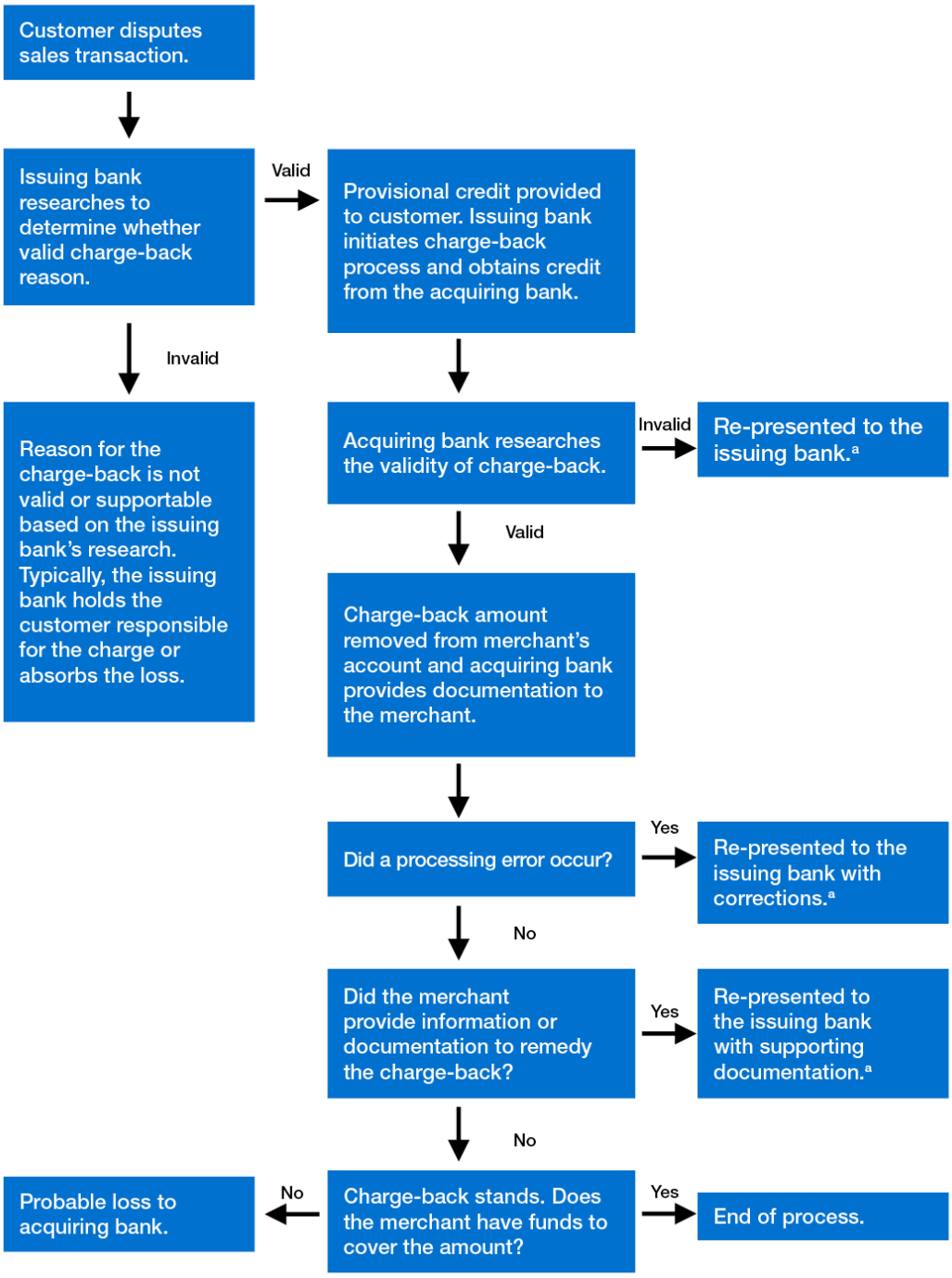
Specific details regarding all of the consumers' rights and responsibilities can be found in the "Electronic Fund Transfer Act" booklet of the *Comptroller's Handbook*.

The charge-back processing and time frames between the bank and its merchant are generally addressed contractually via the merchant processing agreement.

Figure 3 illustrates the general charge-back process for credit transactions.

[3] The customer has 60 days to report a dispute under federal consumer regulations (12 CFR 1026, "Truth in Lending," known as Regulation Z), but the card association may allow more time to initiate a charge-back.

Figure 3: Charge-Back Process



Source: OCC

[a] The bank card association acts as a payment clearinghouse between the issuing bank and acquiring bank during the charge-back and re-presentment process. A compliance resolution process also exists at the bank card association if no charge-back rights are available to the issuing bank and a financial loss is incurred as a result of bank card association rules.

A second charge-back may occur if the re-presentment is invalid, documentation did not support the charge, or another charge-back reason code applies. If the acquirer disputes the second charge-back presentment, the acquirer may file an appeal for arbitration with the bank card association. Re-presentment is not allowed for a second charge-back.

Card-issuing banks can also initiate charge-backs when the merchant does not follow proper card acceptance and authorization procedures (e.g., no authorization obtained or card used after expiration date). The acquirer incurs contingent liability for as long as 180 days.

Bank card associations have strict charge-back processing rules. For example, an association allows a bank to charge a transaction back to a merchant when the merchant fails to provide copies of the requested sales ticket. If the merchant does not provide a copy of the sales ticket within a prescribed time, the merchant will lose the charge-back dispute. A retrieval request is used by bank card associations to request items from the merchant. The merchant must have a process to respond to retrieval requests and charge-back investigations in a timely manner.

Risks Associated With Merchant Processing

From a supervisory perspective, risk is the potential that events, expected or unexpected, will have an adverse effect on a bank's earnings, capital, or franchise or enterprise value. The OCC has defined eight categories of risk for bank supervision purposes: credit, interest rate, liquidity, price, operational, compliance, strategic, and reputation. These categories are not mutually exclusive. Any product or service may expose a bank to multiple risks. Risks also may be interdependent and may be positively or negatively correlated. Examiners should be aware of this interdependence and assess the effect in a consistent and inclusive manner. Refer to the "Bank Supervision Process" booklet of the *Comptroller's Handbook* for an expanded discussion of banking risks and their definitions.

Merchant processing can be a safe and profitable business if bank management properly understands and controls the primary risks: strategic, credit, and operational. Failure to control these primary risks may result in loss exposures from other risks, such as compliance and reputation.

Strategic Risk

The bank's management must decide whether merchant processing activities are consistent with the bank's overall strategic goals, risk appetite, and business model. If a bank's capital base is limited in relation to existing or projected sales volume, the bank may lack the financial capacity to support the level of risk. Management's internal analysis of capital adequacy and capital allocation for merchant processing activities should comprehensively address all pertinent risk factors.

The OCC expects the bank to have risk management systems commensurate with an activity's risks and complexity. Management experience, staffing, systems, and reporting must be sufficient to enable the bank to monitor merchants and their activities knowledgeably and effectively.

When the board and management of any bank is considering whether to undertake, maintain, or expand a merchant processing business, they must fully understand the risks involved. Business risks should be identified, as well as the expertise and controls required to manage

the risks. Other factors to consider are how well the bank can keep pace with technology and competition, what industries to pursue, and how much to use third-party organizations.

Merchant processing is dominated by a small group of banks with the experience, resources, and infrastructure to process nearly any type and size of merchant, from small Main Street businesses to the largest nationwide retailers. Economies of scale allow these acquirers to compete on service and price, and intense pricing competition and improved and changing technology have resulted in low merchant loyalty, as merchants can change processors virtually overnight.

Banks may be subject to exposure and losses through fraud, charge-back losses, and bank card association fines. The ultimate liability for losses lies with the bank that owns the BIN/ICA number. If the merchant or third-party organization does not have the financial capacity to absorb the loss, the bank must absorb it. The bank that owns the BIN/ICA number is also responsible for compliance with bank card association requirements, including for services provided by a third party. Failure to comply with the bank card association requirements can result in fines, security pledge requirements, and loss of bank card association membership.

Some banks have been financially impaired because of fraudulent and problem merchants signed by ISOs/MSPs. Uncontrolled growth, fraud, and inadequate operations by the third parties have all resulted in significant problems for banks. Before the bank accepts services from an ISO/MSP, it must implement policies, procedures, and controls to monitor the activities of the ISO/MSP and to ensure that the ISO/MSP is operating within the guidelines established by the bank and bank card associations.

Management should evaluate the risks and rewards of whether the bank can process an adequate volume of merchant sales without undertaking an unacceptable level of risk. Large profits at lower volumes can indicate that the bank is processing for high-risk merchants. Significant profits relative to volume levels may also indicate that the bank is using third-party organizations to conduct all activities without expending the resources to manage the business properly.

Deposits from the settlement of merchant processing activities are highly volatile and not a reliable source of funding, especially for a nationwide merchant processing program. A common misconception is that such deposits enable a bank to generate a profitable merchant processing business. In a nationwide program many, if not most, of the merchant-account relationships are at each merchant's primary bank, not the acquiring bank.

Credit Risk

Credit risk arising from charge-backs is a significant risk to an acquirer's earnings and capital. Although processing card transactions is technically not an extension of credit, the acquiring bank is relying on the creditworthiness of the merchant.

Merchant charge-backs become a credit exposure to the acquirer when either the merchant or ISO/MSP declares bankruptcy or is otherwise financially unable to pay. If a merchant or ISO/MSP cannot honor its charge-backs, the acquiring bank must pay the card-issuing bank. Banks have been forced to cover large charge-backs when merchants have gone bankrupt or committed fraud. In many of these cases, the merchant engaged in deceptive or misleading practices. The contingent liability can span several months of the merchant's sales volume because of the cardholder's rights to dispute the charge and the charge-back process. Moreover, high volumes of charge-backs may result in large fines from the bank card associations.

A single merchant or ISO/MSP-related merchants can generate sufficient sales and subsequent charge-backs to result in substantial losses to the bank. Charge-backs from a fraudulent or problem merchant (or group of these merchants) can total hundreds of thousands of dollars per day. These charge-backs can translate into recognized losses to the acquiring bank if the merchant or ISO/MSP is incapable of payment. Charge-back losses can deplete earnings and capital in a matter of days, causing a bank to fail.

Substantial credit risk can arise when an ISO/MSP uses a bank's BIN/ICA number. The indemnification of losses by the ISO/MSP is only as strong as the creditworthiness of the ISO/MSP and the creditworthiness of the merchants signed by the ISO/MSP. Many of the most serious merchant processing losses at banks have resulted from merchants solicited by ISOs/MSPs (even when ISOs/MSPs were contractually responsible for losses).

If an acquiring bank permits other bank card association members to use its BIN/ICA number, it also assumes credit risk. The BIN/ICA number owner has primary responsibility to the bank card association for any user's (user of the BIN/ICA number) failure to perform. Using another member's BIN/ICA number is also risky. If the bank owning the BIN/ICA number fails to perform, the bank card association may hold the users of the BIN/ICA number liable. Although sharing BIN/ICA numbers is less common than in the past, users could be liable for all activity involving the BIN/ICA number if they are members of the bank card associations.

Operational Risk

Acquiring banks are faced with operational risk daily as they process card transactions for their merchants. This risk arises primarily from the settlement process. Settlement is the process of transmitting sales information to the card-issuing bank for collection and reimbursement of funds to the merchant. Operational risk can also arise from a bank's failure to process a transaction properly, inadequate controls, employee error or malfeasance, a breakdown in the bank's computer system, or a natural catastrophe.

Among the operational risk exposures are processing risks. A failure anywhere in the transaction process can result in risks to the bank's earnings and capital. For example, the failure to

- monitor the merchant acceptance process (including merchant acceptances generated by ISO/MSP relationships) can result in significant operational and credit problems. These include possible bank card association fines; credit, fraud, and operational losses; inadequate staffing and infrastructure; and reputation repercussions.
- process charge-backs properly and in a timely manner, as specified in the bank card association rules, can result in operational and credit losses.
- provide adequate staffing for charge-back processing and fraud monitoring can result in preventable operational and credit losses that occurred because of high workloads. Workloads can change quickly depending on sales growth and charge-back volume.
- comply with bank card association operating rules can bring substantial fines.
- monitor daily sales transactions can result in substantial operational losses from fraudulent activity.
- provide or the inability to provide timely transmission of funds to merchants or third parties can result in operational losses, reputation risk, and liquidity risk.
- monitor the service quality and fulfillment (e.g., sales, charge-back processing, fraud monitoring, customer service, or ACH file creation) provided by third-party organizations can result in operational and credit losses, fines, and a negative reputation.
- monitor and compare initial merchant activity and pricing with actual merchant activity and pricing can result in unprofitable operations.

In addition, there is risk in all outsourcing arrangements, because the bank must ensure that the chosen service provider complies with all guidance and regulations and has policies and procedures that reflect those of the bank.

Operational risk exposures arise from the hardware and software used for processing, if there are intrusions or negative alterations, internally or externally. The same is true for the transaction data that is handled in processing. Risk also arises if the data is not accessible for necessary monitoring and reports. Operational and compliance risks arise if personally identifiable information emerges from the merchant processor as a result of social engineering or a cyber attack.

Although data may not be expropriated, cyber attacks can cause degradation or even complete disruption of services to customers, alteration of customer data, and in the worst case, they could lead to the destruction of systems and customer data. Data stored or data in transmission is at risk.

Fraud risk is another operational risk. Fraud can exist in any part of the payment transaction and thus creates a risk exposure for the merchant processor. Fraud at the authentication level is often referred to as identity theft. Fraud at the authorization level may be caused by cyber attacks or complicity with a merchant or merchant employee.

Compliance Risk

Compliance risk may occur in various parts of offering and providing the merchant processing activity. While the risk may occur at the bank level, this risk can also exist when products, services, or systems associated with a third-party relationship are not properly

reviewed for compliance, or when the operations of the third-party relationship are not consistent with law, ethical standards, or the bank's policies and procedures.

The potential for serious, frequent violations or noncompliance is heightened when a bank's oversight program does not include appropriate audit and control features, particularly when the third-party organization is implementing new bank activities or expanding existing ones. Compliance risk also increases when the privacy of consumer and customer records is not adequately protected, when conflicts of interest between a bank and affiliated third parties are not appropriately managed, and when a bank or its service providers have not implemented an appropriate information security program. Banks should involve their compliance management function in the due diligence and monitoring process, because third-party products or services present significant risk to regulatory compliance.

Banks are required to have Bank Secrecy Act/Anti-Money Laundering (BSA/AML) compliance programs and appropriate policies, procedures, and processes to monitor and identify unusual activity. The OCC expects banks to effectively assess and manage risks, including those presented by third-party organizations (such as processors). Processors are generally not subject to BSA/AML; as a result, some processors may be vulnerable to money laundering, identity theft, fraud schemes, and illicit transactions or transactions prohibited by the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC).

The bank's BSA/AML risks when dealing with a processor account are similar to risks from other activities in which a bank customer conducts transactions through the bank on behalf of the customer's clients. When the bank is unable to identify and understand the nature and sources of the transactions processed through an account, the risks to the bank and the likelihood of suspicious activity can increase. If a bank has not implemented an adequate processor approval process that goes beyond credit risk management, it could be vulnerable to processing illicit or OFAC-sanctioned transactions.

Banks are required to have Graham-Leach-Bliley Act (GLBA) compliance programs and appropriate policies, procedures, and processes to safeguard confidential customer information. The GLBA introduces additional legal/compliance risk due to the potential for regulatory noncompliance in safeguarding customer information. The bank's GLBA risks when dealing with a third-party processor that possesses confidential customer information are the same as the risks when the bank possesses the information. The potential exists for legal liability related to customer privacy breaches.

Inadequacies in compliance with laws and regulations, policies and procedures, and ethical standards may subject the bank to litigation and legal expenses. The bank should verify, directly or through a processor, that the merchant is operating a legitimate business. Such verification could include comparing the identifying information against public record and fraud databases; comparing the identifying information with information from a trusted third party, such as a credit report from a consumer reporting agency; or checking references from other banks and other financial institutions.

Reputation Risk

The bank must consider the possible reputation risks involved in merchant processing. Should any interaction and aspect of merchant processing conducted by the bank or its third-party organizations not be consistent with the bank's policies and standards, the bank could be subject to reputation risk. Publicity about adverse events surrounding third-party organizations may increase the bank's reputation risk. Decisions made by the bank or third parties acting on the bank's behalf can directly cause the loss of merchant relationships, litigation, fines and penalties, and losses associated with charge-back reimbursements.

Banks that use third-party organizations to offer new products or services or expand existing ones must closely monitor the quality and appropriateness of the provider's products and services to ensure ongoing customer satisfaction. Furthermore, the acquirer must perform strong due diligence of new third-party organizations and ongoing evaluation of third-party service standards and financial stability.

Risk Management and Controls

The OCC expects each bank to identify, measure, monitor, and control risk by implementing an effective risk management system appropriate for its size and the complexity of its operations. When examiners assess the effectiveness of a bank's risk management system, they consider the bank's policies, processes, personnel, and control systems. Refer to the "Bank Supervision Process" booklet of the *Comptroller's Handbook* for an expanded discussion of risk management.

This section focuses on the primary methods by which acquiring banks, agent banks, and referral banks manage and control risk. The risk management processes and controls may vary from bank to bank.

Board and Management Supervision

The board and management must ensure the bank has a comprehensive risk management framework in place commensurate with the bank's complexity and risk profile. The framework should enable the bank to assess, measure, monitor, and control the various individual risks associated with the bank's merchant processing activities (as discussed in the "Risks Associated With Merchant Processing" section), or risks within lines of business or by function, as well as assess these risks in aggregate with other risks across the banking enterprise. The importance and need for a comprehensive and integrated approach to risk management has increased in an environment that has become more complex. This complexity is reflected in: (1) the structure of many banks; (2) the products and services being developed; (3) the technology being used to deliver products and services and to interface with consumers; (4) the competition in the marketplace; and (5) the global presence of many banks. Consequently, the importance and value of an enterprise approach to risk management cannot be overstated.

The bank's risk management process should include written policies and procedures appropriate to the size and complexity of operations. Risk management must include a system for approving merchants and an ongoing program to monitor their credit quality and guard against merchant fraud or sanctioned activity. The board and management must establish a sound internal control environment and audit culture. In addition, the board of directors, acting through senior management, is ultimately responsible for ensuring that the bank maintains an effective internal control structure that includes suspicious activity monitoring and reporting.

Management and staff should have knowledge and skills appropriate for the type and level of the risk the bank takes. For example, personnel responsible for processing charge-backs should fully understand bank card association rules, and personnel responsible for approving merchant applications should be able to properly evaluate merchant creditworthiness and identify high-risk merchants. Staffing levels should be commensurate with the workload.

Risk measurement technology systems must be in place to operate, monitor, and control the activity effectively. The board and management should regularly receive reports that enable them to gauge the department's risk. Key management reports should detail new account acquisitions, account attrition, portfolio composition, sales volumes, charge-back volumes, charge-back aging, fraud, suspicious activity reporting, sanctions screening, and department profitability.

Agent Banks

Agent banks should fully understand their financial liability for merchants' charge-back and fraud losses and their responsibilities under the agreement with the acquirer. Agent banks with liability should establish appropriate risk controls, including ongoing monitoring. Monitoring should include sales activity, charge-backs, and fraud investigations.

Referral Banks (Agent Banks Without Liability)

Referral banks generally need no more than modest controls to monitor their relationship with the acquirer. If management has made any indemnification agreements or other commitments, however, more comprehensive controls and reporting should be established because the referral bank is exposed to liability.

Capital Allocation and Limits

The bank should hold appropriate capital for merchant processing activities, based on the level of risk associated with the activity. Any higher risk posed due to a contractual arrangement with a third-party organization for merchant processing activities should be considered when determining the adequacy of capital for the activity. The board and management should limit the bank's volume of merchant processing relative to its capital, its risk profile, and management's ability to monitor and control the risks of merchant processing. The board-approved policy governing merchant processing should require at

least an annual analysis of capital allocated for merchant processing activities, and the analysis should be approved by the board.

Factors to consider in connection with merchant processing include

- current and expected sales volume
- merchant type and location.
- role and supervision of third-party organizations.
- management expertise.
- ability to identify, measure, monitor, and control risks.
- skill of personnel.
- charge-back level.
- merchant processing profitability.
- bank's risk profile.
- adequacy of capital to support other lines of business.

Management must consider the implications for capital of off-balance-sheet risk (e.g., fraud and charge-back exposure resulting from transactions, sales volume, and higher-risk merchants). Both operational and credit losses can occur quickly. The bank must determine whether its financial resources are adequate for the risk exposure of merchant processing and the potential impact of the activity on earnings and capital.

Existing regulations do not assess a specific capital charge for merchant processing activities, but capital regulations (12 CFR 3, subpart H) generally permit the OCC to require additional capital to support the bank's risk level. Depending on the risk profile of the bank's merchant processing activities, the OCC may require capital above the regulatory minimums to support the risks of merchant processing. See OCC Bulletin 2012-16, "Guidance for Evaluating Capital Planning and Adequacy," for OCC expectations regarding capital adequacy and guidance on capital planning. The guidance also addresses various actions the OCC may take to ensure that the bank's capital planning process and capital level remain adequate for its complexity and overall risks.

Specifics vary, but bank card associations have definitive rules that limit the processing volume a member can generate relative to its capital, concentrations of high-risk merchants, and charge-back rates. The OCC, however, may require more restrictive limits, consistent with safety and soundness, than the bank card associations impose. Examples of requirements that associations may impose include the following:

- **High-risk merchant concentration:** Proportion of aggregate merchant sales volume comprising merchants in high-risk merchant activities. The bank also may have established a target maximum percentage limit for this concentration.
- **Capital support for charge-backs:** Aggregate charge-backs for the previous six months as a proportion of the bank's tier 1 capital. The bank also may have established a maximum percentage limit for this calculation.

- **Capital support for merchant sales volume:** Average weekly merchant sales volume for the most recent quarter divided by the bank's tier 1 capital. The bank also may have established a minimum tier 1 capital level as a percentage of weekly sales.

Board and management should have full knowledge and understanding of the associated capital and collateral obligations that may exist for the bank's merchant processing activities, as well as any other credit mitigation instruments such as letters of credit or guarantees. Also, any collateral obligations for the activity should be reported to the board and management on a regular basis.

Security Pledges

Bank card associations may require security pledges to protect the bank card payment system. These security pledges can be large if the risk posed by the bank's merchant processing activities is high. Management should fully understand that the bank card associations may have contractual rights to offset funds from the bank's settlement account without the bank's prior permission.

Payment Card Industry Security Standards Council

The Payment Card Industry (PCI) Security Standards Council was founded in 2006 by the major payment card brands: American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa. The council is a global open forum that is responsible for the development, management, education, and awareness of the PCI Data Security Standard and other standards that increase payment data security. As of November 2012, the council had over 600 participating organizations representing merchants, banks, processors, and vendors worldwide. Although the PCI standards are not established or endorsed by the OCC, the standards may help the bank manage operational risk.

PCI Security Standards

The PCI Security Standards are technical and operational requirements the council sets to protect cardholder data. The standards are global and govern all merchants and organizations that store, process, or transmit payment data, and include specific requirements for software developers and manufacturers of applications and devices used in the transaction process. Compliance with the standards is enforced by the major payment card brands that established the council.

PCI Data Security Standard for Merchants and Processors

The PCI Data Security Standard (PCI DSS) for Merchants and Processors is the global data security standard that a merchant must adhere to in order to accept payment cards. The standard includes the following six goals and 12 requirements:

- Build and maintain a secure network.

  - Requirement #1: Install and maintain a firewall configuration to protect cardholder data.
  - Requirement #2: Do not use vendor-supplied defaults for system passwords and other security parameters.
- Protect cardholder data.
  - Requirement #3: Protect stored data.
  - Requirement #4: Encrypt transmission of cardholder data across open, public networks.
- Maintain a vulnerability management program.
  - Requirement #5: Use and regularly update antivirus software or programs.
  - Requirement #6: Develop and maintain secure systems and applications.
- Implement strong access control measures.
  - Requirement #7: Restrict access to cardholder data by business need-to-know.
  - Requirement #8: Assign a unique ID to each person with computer access.
  - Requirement #9: Restrict physical access to cardholder data.
- Regularly monitor and test networks.
  - Requirement #10: Track and monitor all access to network resources and cardholder data.
  - Requirement #11: Regularly test security systems and processes.
- Maintain an information security policy.
  - Requirement #12: Maintain a policy that addresses information security for all personnel.

PCI DSS attempts to establish essential practices for securing cardholder data. If security control requirements are not properly implemented, data breaches may occur. Significant deviations from PCI DSS may result in security breaches. PCI DSS compliance is not, however, a guarantee that breaches will not occur.

Merchant Underwriting and Review

Management should implement a formal merchant underwriting and approval policy to control credit risk. The policy should designate the types of merchants with which the bank is willing to conduct business as well as the criteria for selecting merchants (e.g., time in business, location, and sales volumes). Further, the bank's policy should define what information each application should contain, such as type of business, location, and Social Security number/tax identification number for the business entity or principal owners. The policy should also stipulate what information is required in the merchant agreement. The merchant agreement should disclose all fees, define what the merchant is required to do at point of sale, and require notification of ownership changes or substantive marketing and product changes. The policy also should outline the procedures and schedules for the periodic reviews of the financial status of the existing merchant base.

Underwriting Standards

The underwriting policy should require a background check of the merchant to support the validity of the business, creditworthiness of the merchant, and sales history. The bank's underwriting standards should require, at a minimum,

- signed application.
- signed processing agreement.
- signed corporate resolution, if applicable.
- adequate understanding of the merchant's business to ensure that it is classified under the merchant category code.
- on-site inspection report or verification of business.
- credit bureau reports, as allowed by the Fair Credit Reporting Act, on the principal of the business.
- financial statement or credit reports on the business.
- analysis of the merchant's activity based on recent monthly statements from the merchant's current or most recent processor, if available.
- Paydex score provided by Dun and Bradstreet, if available for additional information to consider (the OCC does not endorse particular products or vendors).
- verification of trade and bank references.
- evidence that the merchant is not on OFAC's Specially Designated Nationals List (SDN List) or the bank card industry's Member Alert to Control High Risk Merchants (MATCH) list. Such checks are standard industry practice.

Review and Approval of Merchants

In the initial review of a merchant application, the bank should reject a merchant with a history of substantial charge-back volumes, weak financial condition, or failure to operate a valid business. The depth of the initial review should match the level of risk the merchant poses. Many acquirers are moving toward a risk-based approach to merchant underwriting. Lower-risk or lower-volume merchants may require only a limited underwriting process while higher-risk merchants undergo far greater analysis. Acquirers using risk-based underwriting typically use enhanced credit and fraud monitoring systems.

The bank should also establish criteria for reviewing applications from a merchant's other locations (if the merchant conducts business in more than one location). These procedures may be abbreviated from the standard underwriting guidelines, but verification is necessary. Verification should ensure that the type of business is similar to the existing location's and that the merchant owns the additional locations.

The bank should establish who can approve new accounts. To approve a merchant with a high sales volume, a senior officer's authorization should be required. Commercial lending experts should assess the creditworthiness of large merchants.

The policy should address documentation requirements. If the acquiring bank uses information collected by the ISO/MSP, the bank's policy should outline the quality of information required and the review procedures required.

Prohibited or Restricted Merchants

When evaluating merchants' credit quality, banks must consider the business lines and any products the merchants offer. The bank card associations segment businesses by activity, and acquiring banks should analyze merchants along similar lines on an ongoing basis. Most acquiring banks compile lists of prohibited or restricted merchants, describing the types of merchants they are unwilling to sign or are willing to sign only under certain circumstances.

Certain types of businesses are inherently more risky. For example, although there are many reputable mail order and telemarketing (often called MO/TO or MOTO) merchants, these merchants have, in aggregate, displayed a much higher incidence of charge-backs. Also, the risk of charge-back is greater if the merchant sells goods or services for future/delayed delivery, such as airline tickets, health club memberships, or travel clubs. In such circumstances, customer disputes are not triggered until the date of delivery.

Many banks use holdback or reserve accounts to mitigate credit risk on higher-risk merchants.

Internet Merchants

The Internet gives fraudulent businesses and businesses with minimal financial resources ready access to the public. Acquirers should conduct thorough underwriting reviews of Internet merchants using bank and trade verifications. During the underwriting process, credit analysts should determine whether heightened fraud and charge-back risks warrant the use of additional risk mitigation techniques, such as delaying settlement or establishing reserves.

Electronic commerce and the use of the Internet pose privacy and security concerns that should be addressed in the initial underwriting. The bank should ensure the security of transactions as well as stored data. Secured servers and data encryption technologies help to protect data and transaction integrity.

For Internet merchants, underwriting standards should stipulate that the following information must appear on the Web site:

- Customer service number (toll-free is preferable).
- If the Web site or merchant uses an alias, the actual name of the entity that operates or controls the merchant.
- E-mail address to contact the company.
- Statement on security controls.
- Delivery methods and timing.
- Refund and return policies.

- Privacy statements (permissible uses of customer information).

Concerns regarding potential fraudulent businesses with minimal financial resources, as well as data and transaction integrity, are not limited in the merchant world and may occur regardless of the method and location of the merchant sales. While there are still monoline Internet merchants, many brick-and-mortar (storefront) merchants also provide Internet sales. Conversely, there are also traditional merchants that have morphed into primarily Internet-based operations, versus the brick-and-mortar operations of the past.

Periodic Review

The financial condition of high-volume and high-risk merchants should be regularly monitored. The bank's policy should stipulate the frequency of reviews and the size of merchants requiring reviews. In determining the threshold for periodic reviews, the bank should consider volume, concentrations, high-risk industries, and charge-back history. Depending on the composition of the bank's portfolio, it may not be necessary for the bank to review smaller merchants periodically; the bank may be able to rely on sound underwriting guidelines at acquisition. Whether or not a merchant's credit is reviewed periodically, its transactions—and those of every merchant—should be monitored rigorously for such events as fraud, charge-backs, suspicious activity, and sanctioned activity. To screen portfolios periodically for troubled accounts, many acquirers now use information databases (e.g., databases of risk scores, bankruptcy filings, and fraud data).

When a bank's merchant processing department and its commercial lending department each have a relationship with a merchant, each should inform the other department about any change in the merchant's credit quality. For example, a merchant's unacceptable charge-back rate could indicate emerging problems of credit quality, and a merchant's problem loan may signal increased risk with the merchant relationship. The bank should include the merchant manager on the routing of the problem loan report. If credit information shows that the merchant's financial condition is deteriorating, the bank may want to reduce its risk exposure. For instance, when dealing with a financially unstable merchant, the bank may require a holdback reserve or security deposit.

Acquiring Bank Reviews of Agent Banks

Acquiring banks should periodically review the financial condition of agent banks that assume loss liability. The financial capacity of the agent bank should be consistent with the risk profile of its merchant portfolio and volume of merchant activity. The acquirer does not need to review periodically a referral bank's condition.

Agent Bank Merchant Underwriting

Agent banks with liability should have appropriate underwriting procedures in place. The acquiring bank expects the agent bank to reimburse it for any losses sustained. The agent bank's management should refer to the acquiring bank's underwriting criteria when developing guidelines. Acquirers may decline merchants that agent banks refer if the

merchants pose undue risk or do not meet the acquirer's minimum standards for merchant underwriting.

The complexity of an agent bank's underwriting guidelines will depend on the type of merchants it targets. If the account base is limited to existing customers and sales volumes are low, written underwriting guidelines may be minimal. When accounts are high risk or volume is high relative to the bank's capital base, more extensive guidelines are appropriate. Agent banks often have more stringent criteria for nonbank customers, who the banks may be less familiar with, than for existing bank customers.

Profit Analysis and Monitoring Pricing

To ensure that the pricing process is adequately controlled, a bank's pricing policies should address the methods used for pricing, authority levels, and repricing procedures. The pricing policy facilitates consistency in pricing practices and helps optimize profit margins.

Management should ensure that merchants are priced appropriately throughout the life of the contract. The bank should verify a merchant's projected volume and average ticket size shortly after processing begins and periodically thereafter and should ensure that the initial discount rate is in line with the application estimate and original pricing model assumptions. All significant merchants should be reviewed for repricing at least annually, and if any merchants are unprofitable, they should be repriced. Most agreements allow acquirers to increase discount rates and fees at any time during the life of the contract.

Banks must have management information systems (MIS) in place to measure the profitability of the merchant processing department. The quality of MIS varies among banks. Information systems should detail key performance measures such as net income to sales and net income per item. Ideally, the banks should be able to segment profitability by merchant, acquisition channel, risk exposure, and industry.

An acquiring bank's merchant operation should produce a discrete income statement. The income statement should include all direct and indirect costs. Direct costs include internal data processing, merchant accounting, fraud and charge-back losses, personnel, and occupancy costs. Indirect costs may include corporate overhead expenses such as human resources, legal, and audit services. Refer to appendix C of this booklet for a sample profit and loss statement.

Management and the board should be kept informed of the merchant processing department's profitability. The level of detail and frequency of reporting to the board is contingent on the size and risk profile of the operation in relation to the overall operations of the bank and its capital base.

By implementing effective and appropriate controls over processors and their merchant clients, a bank should be able to identify those processors that process fraudulent transactions for merchants to ensure that the bank is not facilitating these transactions. In the event that a bank identifies fraudulent or other improper activity with a processor or specific merchant,

the bank should take immediate steps to address the problem including filing a Suspicious Activity Report (SAR) when appropriate, terminating the bank's relationship with the processor, or requiring the processor to cease processing for that specific merchant.

Agent Bank Pricing and Profitability

An agent bank's pricing should be sufficient to recoup the fees charged by the acquirer as well as the agent bank's other costs. Depending on the size of the agent bank's merchant portfolio, separate profitability reports on this line of business may not be necessary. Management should always be able to determine whether the service is profitable to the bank. If profits are insufficient, management should consider whether other benefits of offering merchant processing services make up the difference.

Member Alert to Control High-Risk Merchants

MATCH is an identification system that logs merchants and principals (the owners of the merchant business) terminated for specific reasons. When acquiring banks and transaction processors terminate contracts with merchants for certain risk-related reasons, the merchant businesses and their owners should be placed on MATCH. The listing on MATCH indicates that the merchant committed one or more specific acts that convinced the acquiring bank or processor that the acceptable level of risk had been exceeded.

The specific reasons or types of acts that would warrant the merchant being placed on MATCH include

- excessive charge-backs due to merchant business practices or procedures.
- excessive deposits for transactions unauthorized by cardholders.
- credit or debit card fraud conviction.
- excessive deposits for counterfeit transactions.
- deposits for transactions involving sales of goods or services generated by another merchant (laundering or factoring).
- suspicion that the merchant is conducting fraudulent activity.

It is not uncommon for merchants to be placed on the list for technical violations of their merchant agreements, which would not be considered risk-related reasons, or possibly for several charge-backs that did not cause the processor a loss, or that may not have exceeded an acceptable level of risk.

The MATCH list is accessed more frequently by banks for investigating new merchant account applications than for reporting possible felonious merchants. Using the MATCH data to review merchant applications should be the starting point in the process. The inquiring bank should always base its acceptance decision for a new merchant account on its own firsthand investigation and due diligence process.

MATCH is maintained by MasterCard International and used by MasterCard, Visa USA, and American Express.

Fraud Monitoring

Detection Methods

Issuers are primarily responsible for fraud monitoring, but merchant fraud detection systems may help identify cardholder fraud through transaction monitoring. Bank card associations prepare fraudulent activity reports for acquiring banks. These reports should be used in coordination with a bank's fraud system as verification. Bank card associations may require acquiring banks to document plans to correct unacceptable merchant sales practices. Additionally, associations provide educational material to acquirers and merchants regarding the latest techniques in fraud detection.

Issuing banks also must monitor for fraud by merchants. Fraud analysts should not rely exclusively on excess charge-back activity to identify fraud. The primary tool for detecting merchant fraud is an exception report that details variances from parameters established at account setup. Basic parameters may include daily sales volume, average ticket size, multiple purchases of the same dollar amount, multiple use of the same cardholder number, the percentage of transactions keyed versus the percentage swiped, and charge-back activity. A daily exception report lists the merchants that breach these parameters.

Most large-volume processors have exception parameters by industry or merchant type. To maximize the efficiency of staff and monitoring reports, the bank should periodically review and update parameters as necessary. The daily sales threshold may be set at a percentage (e.g., 110 percent) of the activity in a prior time frame (e.g., three months' average). Such a margin allows for normal merchant growth and compensates for seasonal sales patterns. Internet merchants may require a higher level of monitoring because of heightened fraud and charge-back risks associated with this sales channel. Banks should develop monitoring for Internet-based merchants commensurate with the risks associated with these merchants.

Many acquirers take advantage of developments in neural network technology. Firms marketing such products have designed complex computer programs that compare each transaction against the merchant's prior sales patterns. Such sophisticated products may be beyond the budgets of smaller merchant processors. Some acquirers may selectively route higher-risk transactions through the neural network, subjecting the remaining sales volume to exception reporting.

Many banks use scoring, bankruptcy, trade, and fraud databases to identify merchants that are more likely to falsify transactions because of weak finances or legal difficulties.

Investigations

Bank management should take swift action when it encounters suspicious sales. Its investigation may include verifying purchases with the card-issuing bank or obtaining copies of paper-based transaction tickets from the merchant. An acquirer's quick response helps to minimize losses for the acquirer and the card-issuing bank, as well as to notify law

enforcement agencies. Daily staffing should be sufficient to determine whether any of that day's exceptions has the characteristics of a fraudulent transaction.

Merchant agreements should allow the acquirer to delay settlement of funds until questionable transactions are resolved. Once fraud is suspected, management must file a SAR with the Financial Crimes Enforcement Network (FinCEN). Additionally, the account of a fraudulent merchant should be terminated, and the merchant's business and their owners should be placed on the MATCH list.

Charge-Back Monitoring

An acquirer must have strong controls in place to accurately process charge-backs and retrieval requests in a timely manner. The acquirer may lose a charge-back dispute (and lose the money involved) if it does not adhere to strict bank card association rules. The bank card associations notify acquirers of merchants having excessive charge-backs, which may be based on volume, amount, or both. The associations may fine banks that have high levels of charge-backs or that do not handle charge-backs properly. Management can limit the charge-back compliance risk by establishing a structured charge-back processing system to monitor and handle merchant charge-backs.

An acquirer's risk management practices should detect merchants having high levels of charge-backs. Numerous charge-backs may indicate an unscrupulous merchant, or the merchant's need for additional training. Employees that monitor charge-backs should be alert for merchants with excessive retrieval requests or charge-backs.

Larger merchant processors employ collectors to recover charge-back losses and other fees. A collector seeks remedy from the principals of the business through negotiations or civil action.

Risk Mitigation

To protect themselves from merchants that pose high risk or that have a history of charge-backs, many acquirers establish merchant reserve accounts or holdback reserves. Holdback reserves are also used to limit a bank's credit risk when the merchant's product or service involves future/delayed delivery. A bank can fund the reserve by setting aside a lump sum or by withholding a portion of each day's proceeds until a specific balance has been reached.

The bank may also fund a general reserve account, similar to the allowance for loan and lease losses (ALLL), for a portfolio of merchant accounts. Although similar to the ALLL, the general reserve for merchant losses should be classified as an "other liability" account and not commingled with the ALLL. The amount of the reserve is often based on the entire portfolio's contingent charge-back exposure. Accounting for the reserve should be in accordance with generally accepted accounting principles.

Banks can also purchase insurance against charge-backs. This insurance is written as comprehensive protection against uncollectible charge-backs. Although the insurance is

comprehensive, banks must follow strict guidelines to collect on the insurance in the event of loss. The insurance can cover nondelivery of the product; unauthorized mail order or telephone order transactions; use of counterfeit, lost, or stolen card numbers; the factoring of credit card transactions; misuse of cardholders' funds; misrepresentation on the merchant application; collusion between the independent sales representative and merchant; and merchants' deceptive and misleading methods of soliciting funds from cardholders.

Accounting and Reporting

Bank management should ensure that charge-back losses are appropriately detailed on call reports as other noninterest expense. Any collected funds are to be reported as other noninterest income. Any uncollectible fees should be reversed from income in a timely manner.

Settlement Controls

Acquiring banks must understand and assess the risk regarding payments and settlement controls from merchant processing activities. An assessment of payments and settlement controls should help management to understand the risks to the bank; to establish policies, procedures, and controls appropriate to these risks; and to develop an audit process to review compliance with policy.

Acquiring banks should have strong vendor management programs that include written agreements with all third-party organizations involved in the settlement process. The agreements should detail responsibilities, payment arrangements and schedules, and contingency plans. Additionally, management should have proper monitoring controls in place over parties in the settlement process. Controls should include quality assurance, audits, on-site visits, performance reporting, and financial monitoring.

Bank management should periodically review settlement transmission reports for large merchants. These reports summarize the interchange rates charged by the bank card associations for each transaction. The reports may assist in identifying merchants with abnormal interchange rates. Abnormal interchange rates may indicate problems with the merchant's terminals or software. Identifying and correcting the problems may result in savings for the merchant and acquiring bank.

The success of settlement controls and payments depends on the participants' (bank, processors, and merchants) credit quality and the system's operational reliability. Management may obtain third-party reviews from its processors. Also, management may request a copy of regulatory examination reports of its processor from the bank's primary regulatory agency.[4] Bank management should refer to OCC Banking Circular 235,

[4] Some services provided to banks by service providers are examined by the FFIEC member agencies. Regulatory examination reports, which are only available to financial institutions that were clients of the service provider when the exam was performed, may contain information regarding a service provider's operations. Regulatory reports are not, however, a substitute for a bank's due diligence, audit, or oversight of the service provider.

"International Payment Systems Risk"; OCC Bulletin 2013-29, "Third-Party Relationships: Risk Management Guidance"; and the *FFIEC IT Examination Handbook* booklets "Outsourcing Technology Services" and "Retail Payment Systems" for guidance in monitoring payment system risks.

Pricing

In general, merchant pricing is extremely competitive, especially for large and national-scale merchants that generate high transaction volumes. The acquiring bank may use various methods to price the merchant account. Smaller merchants are frequently priced with a single discount rate, rather than a range of discount rates, based on merchant volume and average sales ticket. Acquiring banks frequently use unbundled pricing for their medium-size and large merchants. When pricing is unbundled, a fee is charged separately for each service. Fees on interchange, authorizations, and charge-backs may be unbundled. Banks also may unbundle fees for statement preparation, application, customer service, membership, maintenance, and penalty fees (for violation of association rules or for fraud loss recovery due to a data compromise).

The pricing method chosen for a specific merchant should take into account the level of risk the merchant poses. Pricing for higher-risk merchants (e.g., card not present, delayed delivery) may be set higher than for lower-risk merchants.

Many acquirers use pricing models to determine their target discount rates. Acquirers may maintain several pricing models. The model used depends on criteria in the bank's pricing policy, such as the merchant's sales volume or type of business. Pricing models allow acquirers to input different variables for different sales volumes, average sales tickets, revenue, or expenses, and such adjustments are designed to produce desired profit margins. The pricing model should include all direct and indirect expenses. The accuracy of any pricing model depends on reasonable assumptions for revenue and expenses.

Discount Rate

The acquiring bank assigns a discount rate to the merchant account at the time the merchant agreement is signed. In the simplest case, the discount represents a single rate charged a merchant based on the individual merchant's sales volume. For example, a merchant with a 2 percent discount rate receives $98 for a $100 credit card sale processed with the acquiring bank. The discount is generally charged monthly to the merchant. This creates a timing difference because the bank is settling interchange with the bank card associations daily. In other words, the bank in most cases pays the interchange charges before receiving payment for these charges from the merchant. This timing difference creates a credit exposure for the bank on the discount payable from the merchant.

Most merchant agreements allow the acquiring bank to change the discount rate for various cost increases. The most typical change is passing along new interchange rates set by the bank card associations. The discount rate generally ranges from 1 percent to 4 percent for small to medium-size merchants. Discount rates for high-volume merchants may be less than

1 percent, and many large merchants receive (are priced using) unbundled pricing rather than discount rates. Merchants using electronic data capture systems**,** which are cheaper and more accurate**,** are charged lower discount rates than merchants that generate paper-based transactions.

The bank's managers should be able to explain major deviations from minimum discount rates. Banks often give a favorable discount rate to merchants that are commercial borrowers or deposit holders. A merchant's discount rate can also be favorable because the merchant leases card equipment from the bank. Although setting prices based on other services or relationships is an acceptable practice, the bank should be able to measure the overall profitability of a merchant account. The bank examiner should review discount rates for insiders and affiliates to ensure that they do not receive better rates and terms than similar bank customers.

Interchange Fees

An interchange fee is paid by the acquiring bank to the issuing bank via bank card associations for the transaction passing through interchange. Therefore, interchange is an expense on the acquirer's income statement and income on the issuer's income statement.

Bank card associations set interchange rates on a periodic basis (generally on an annual basis and usually in April). There are numerous interchange rates relating to factors such as the type of authorization (e.g., card present or card not present) and type of business (e.g., grocery store). The acquiring bank must consider the different interchange rates when pricing merchants.

Processing Fees

The processing fee varies with the size and number of transactions the merchant submits per batch, and covers the costs associated with data-processing services required for the transactions. The processing fee may include data capture and authorization costs. The fee may go directly to the bank if it does all of the processing or to the bank's third-party processor.

Termination Fees

A merchant-account contract may require a termination fee payable by the merchant. Some merchant-account contracts require that the term of the contract last a certain length of time (e.g., one or two years), while some may not. When a termination fee is part of the contract, and the merchant terminates the contract early, the merchant is required to pay the termination fee. Depending on the volume level of the merchant's activity on the account and the bank's policy, the merchant may negotiate to have the termination fee waived.

ISO/MSP Fees

The ISO/MSP fee is the amount the acquiring bank pays the ISO/MSP for services provided. These services usually include soliciting merchants and customer service. The fee is negotiated and often represents a percentage of the volume the ISO/MSP-sponsored merchants bring to the bank. Pricing for the merchant signed by the ISO/MSP should be consistent with the fee agreement between the bank and the ISO/MSP.

Agent Bank Commission

The agent commission is a fee earned by the agent bank for signing a merchant. This fee is built into the discount rate or charged separately.

Other Income

Discount income is not the only way banks generate fee income. Other income-generating programs include equipment leasing, merchant clubs offering unlimited supplies, travel agency services, and term life insurance. Management should make sure that any products and services offered comply with applicable laws and regulations.

Scorecards and Models

A scorecard is a tool for evaluating the potential performance of prospective merchants. While scorecards may vary in design, they focus on specific measures or targets associated with the applicable activity, cause and effect dynamics, financial and nonfinancial components, business processes, growth, and a wide range of other variables. Scorecards may be manual or automated, simple or complex. The more complex the scorecard, the more likely that it is highly automated.

Some scorecards may qualify as models and require adherence to OCC Bulletin 2011-12, “Sound Practices for Model Risk Management: Supervisory Guidance on Model Risk Management.” For purposes of OCC Bulletin 2011-12, “model” refers to a quantitative method, system, or approach that applies statistical, economic, financial, or mathematical theories, techniques, and assumptions to process input data into quantitative estimates. A model consists of three components: an information input component, which delivers assumptions and data to the model; a processing component, which transforms inputs into estimates; and a reporting component, which translates the estimates into useful business information. The definition of model also covers quantitative approaches whose inputs are partially or wholly qualitative or based on expert judgment, provided that the output is quantitative in nature.

Scorecards for merchant processing are generally proprietary. Scorecards may exist for a variety of purposes related to merchants, fraud, and other bank products and services. Banks should adequately assess whether scorecards rise to the level deemed a model per OCC guidance and, if applicable, should adhere to the aforementioned model guidance, which

addresses model risk management; model development, implementation, and use; model validation; and governance, policies, and controls.

Managing Third-Party Organizations

Selecting a Third-Party Organization and Due Diligence

Regardless of the type of third-party relationship, selecting a competent and qualified third-party provider is essential to managing third-party risk. The due diligence process provides the bank with an opportunity to identify qualitative and quantitative aspects, both financial and operational, of a third party and to assess whether the third party can help the bank achieve its strategic goals. Banks should conduct appropriate due diligence before selecting a third party and at appropriate intervals thereafter.

Due diligence should involve a thorough evaluation of all available information about the third party, and may include reviews of

- experience in implementing and supporting the proposed activity.
- audited financial statements of the third party and its significant principals.
- qualifications, backgrounds, and reputations of company principals, to include criminal background checks, when appropriate.
- internal control environment and audit coverage.
- adequacy of MIS.
- business resumption, continuity, recovery, and contingency plans.
- technology recovery testing efforts.
- cost of development, implementation, and support.
- reliance on and success in dealing with subcontractors.
- insurance coverage.

Banks should check the background of each principal of an ISO/MSP. The financial capacity of the ISO/MSP and its principals should also be analyzed to verify the organization's viability and capacity to absorb losses. Many acquirers obtain cash deposits from the ISO/MSP to support the contractual arrangement. Banks should review an ISO's/MSP's financial condition periodically.

Bankers should refer to OCC Bulletin 2013-29, "Third-Party Relationships: Risk Management Guidance," for additional guidance. Also, refer to *FFIEC IT Examination Handbook* booklets "Outsourcing Technology Services" and "Supervision of Technology Service Providers" for additional information.

Contracts

Bank card associations require written contracts between an acquirer and the ISO/MSP. Bank card associations have specific guidelines relating to contract provisions, functions controlled by the acquiring bank, accessibility to procedural audits, and record-keeping requirements. A

written contract should clearly set out the responsibilities of each party, compensation and liability arrangements, allowable uses of the acquiring bank's name, and reasons the contract can be terminated. A bank legal counsel familiar with the specialized nature of merchant processing should review all contracts.

On-Site Inspections, Audits, and Attestation Engagements

Management should periodically conduct on-site inspections and audits of third-party organizations. Audit reports should be generated, and the third-party management should be required to respond to identified issues. If the third party is required to have specialized audits or an attestation engagement (e.g., attestation engagement according to Statement on Standards for Attestation Engagement (SSAE) No. 16, "Reporting on Controls at a Service Organization," or if it elects to have such audits or attestation, management should obtain and review the audits or attestation.

SSAE 16 is an attestation standard put forth by the Auditing Standards Board (ASB) of the American Institute of Certified Public Accountants (AICPA). The SSAE 16 standard is used for reporting on controls at service organizations. Service organizations, for this standard, are defined as organizations providing services to user entities, for which these services are likely to be relevant to the user entities' internal control for financial reporting. SSAE 16 amended and replaced Statement of Auditing Standards No. 70, "Service Organization" (SAS 70), for service auditor reporting on periods ending on or after June 15, 2011.

A global standard for assurance reporting on service organizations, International Standard on Assurance Engagements (ISAE 3402), has been established by the International Auditing and Assurance Standards Board (IAASB). Although SSAE 16 and ISAE 3402 are very similar, several differences exist. Typically, SSAE 16 is the standard used for service organizations located and operating in the United States, while the ISAE 3402 standard is used by all other companies.

Contingency Planning and Business Continuity

Acquiring banks must also ensure that the third-party processor and network providers have contingency plans in place to continue operations in the event of a disaster. If an ISO/MSP is providing the backroom operations, the bank also should ensure that the ISO/MSP has a contingency plan. The bank should request and review contingency plans for third-party processors and network providers periodically to ensure the adequacy and feasibility of the plans. The merchant processing examination should include information technology (IT) examiners to the extent needed to review the adequacy of the contingency plan, as well as the bank's in-house data-processing systems for merchant processing.

For more information, bankers should refer to the *FFIEC IT Examination Handbook* booklet "Business Continuity Planning."

Supervision of Technology Service Providers

A technology service provider (TSP) is a type of third-party organization. The OCC, the Board of Governors of the Federal Reserve System, and the Federal Deposit Insurance Corporation have statutory authority to supervise third-party servicers that enter into contractual arrangements with their regulated financial institutions (12 USC 1464(d)(7), 1867(c)(1)). The Consumer Financial Protection Bureau has authority as described in 12 USC 5514(e), 5515(d), and 5516(e). The National Credit Union Administration does not have independent regulatory authority over TSPs. These regulatory agencies coordinate interagency programs to supervise TSPs through the FFIEC; thus, TSPs are handled in a unique regulatory way.

A bank's use of a TSP to provide needed products and services does not diminish the responsibility of the board and management. They must ensure that the activities of the TSP are conducted in a safe and sound manner, within acceptable risk parameters and in compliance with applicable laws and regulations, just as if the bank were to perform the activities in-house.

The regulatory agencies expect financial institutions to have a comprehensive, enterprise risk-management process in place that addresses vendor management for their relationships with TSPs. The risk-management process should include risk assessments and robust due diligence for the selection of TSPs, contract development, and ongoing monitoring of all TSP's performance. The risk assessment process should consider all business lines in which TSPs engage to ensure that all covered services are effectively included.

For more information, bankers and examiners should refer to the *FFIEC IT Examination Handbook* booklets "Supervision of Technology Service Providers" and "Outsourcing Technology Services."

Loans to Third-Party Organizations

Banks must fully understand the total risk exposure when lending to third-party organizations that perform services for the bank. The risk exposure to the bank is not only the loans but also the contingent liability from merchant processing activities conducted by the third party through the bank's BIN/ICA number, including the risk of charge-backs. The lending relationship also creates a potential conflict of interest. Lending to a third-party organization, such as for working capital, can result in a bank failing to take appropriate action against the third party when problems are identified. For example, the bank may not want to stop processing for the ISO/MSP because it may jeopardize repayment of the bank's loan. As a result, management might continue with a problem relationship, which may increase the problems and subsequent losses.

Prepaid Debit Cards

Banks involved with processing prepaid debit cards deal with a variety of third-party organizations. Prepaid debit cards, even gift cards, may present potential BSA/AML risks.

Banks should ensure they have compliance programs and the appropriate policies, procedures, processes, and systems to identify, measure, monitor, and control applicable risks. Also, banks should be diligent in monitoring and addressing these risks and be cognizant of laws, rules, regulations, and supervisory guidance included in the “References” section of this booklet.

Examination Procedures

This booklet contains expanded procedures for examining specialized activities or specific products or services that warrant extra attention beyond the core assessment contained in the "Community Bank Supervision," "Large Bank Supervision," and "Federal Branches and Agencies Supervision" booklets of the *Comptroller's Handbook*. Examiners determine which expanded procedures to use, if any, during examination planning or after drawing preliminary conclusions during the core assessment.

Scope

These procedures are applicable for both agent and acquiring banks and are designed to help examiners tailor the examination to each bank and determine the scope of the merchant processing examination. This determination should consider work performed by internal and external auditors and other independent risk control functions and by other examiners on related areas. Examiners need to perform only those objectives and steps that are relevant to the scope of the examination as determined by the following objective. Seldom will every objective or step of the procedures be necessary.

Objective: To determine the scope of the examination of merchant processing and identify examination objectives and steps necessary to meet the needs of the supervisory strategy for the bank.

1. Review the following documents to identify any previous problems that require follow-up. Documents include

   - previous examination findings relating to merchant processing and management's response to those findings.
   - work performed by internal/external auditors and credit examiners including reports issued and management's response to significant deficiencies.
   - supervisory strategy and the scope memorandum issued by the bank's Examiner-in-Charge (EIC).
   - work papers from the previous examination.
   - customer complaints and the resolution of those complaints.

2. Obtain and review management information related to the supervision of merchant processing activities. Refer to the sample request letter in appendix B. Management information includes

   - bank's current strategic plan and any other formal plans that relate to merchant processing operations.
   - management's analysis of capital adequacy and/or capital allocated for merchant processing risks.
   - organization chart including each functional area.

- copies of formal job descriptions for all principals of the merchant processing operation.
- résumés detailing experience of principals in the department.
- copies of management compensation programs, including incentive plans.
- copies of the two most recent monthly management reports provided to the board for merchant processing operations.
- copies of all internal and external audit reports issued since the last examination, with any response from management.
- copies of all internal loan review and loan review reports for the merchant processing activity, because the merchant processing business involves the fundamental evaluation of counterparty credit risk with significant merchants, ISOs/MSPs, and Rent-a-BIN partners. This is something the bank should look at annually.
- new merchant report for the previous three months.
- list of board and executive or senior management committees that supervise merchant processing operations, including a list of members and copies of minutes documenting those meetings since the last examination.
- budget for the merchant processing area at the beginning of the year, and budget revisions as of the examination date.
- report on the bank's top 50 merchants by volume.
- most recent list of high-risk merchants, as well as the prior list at year-end, including volume amounts for the high-risk merchants.
- any analysis or documentation supporting the evaluation of high-risk merchants, and description of actions taken concerning the high-risk merchants.
- copies of Visa and MasterCard association standards and copies of all correspondence from these organizations since the last examination.
- correspondence from bank card associations that pertain to the association's evaluation of the bank's capital adequacy and requests for collateral or other credit mitigation instruments, such as letters of credit or guaranties.
- copies of marketing plans for the merchant processing operation overall and by product.
- copies of merchant processing policies and procedures.
- copies of OFAC sanctions screening results.
- a profitability report for the department for the most recent year-end and year-to-date (YTD) and profitability reports by segment.
- list of all insider or affiliate-related merchants who are customers.
- any management reports on merchants' credit risk.
- daily fraud monitoring reports.
- fraud loss and credit loss history.
- copies of SARs filed.
- charge-back aging report and charge-back ratio and trend reports.
- name and address of agent banks and the volume of business for each one by the merchants they referred.
- list of third-party organizations by name, address, and description of service provided.

3. Review call report information, on Schedule RC-L, "Derivatives and Off-Balance-Sheet Items," for YTD merchant credit card sales volume. Consider the following information possibly detailed on the call report schedule:

   - Sales for which the reporting bank is the acquiring bank.
   - Sales for which the reporting bank is the agent bank with risk (i.e., agent bank with liability).

   The above information should be used as an initial step in evaluating the volumes reported relative to historically reported volumes to see if there have been any significant shifts that might suggest a new activity. Also, the above information may be helpful in a capital adequacy analysis (see the worksheet in appendix E). A capital adequacy analysis shows the volume of reported activities in relation to capital.

4. Identify, during early discussion with management,

   - any changes in business activities (e.g., growth, target market, and products).
   - how management supervises merchant processing operations.
   - any significant changes in policies, practices, personnel, staffing, and controls.
   - any internal or external factors that could affect merchant processing operations.

5. Set the examination's scope and objectives, using findings from performing the preceding procedures and from discussions with the bank EIC and other appropriate supervisors. From the following examination procedures, internal control questions, and verification procedures, select the ones necessary to meet those objectives. Note: Examinations seldom require all steps.

6. As examination procedures are performed, test for compliance with established policies, procedures, internal controls, OCC regulations, and OCC issuances. Identify any area with inadequate supervision, undue risk, or increasing risk profile.

7. Coordinate the review with examiners in charge of reviewing IT risks. In discussion with other examiners, ensure that merchant processing functions are addressed in corporate-wide IT policies and procedures (e.g., business continuity planning and information and operational security).

Acquiring Banks

These examination procedures apply to acquiring banks. If the bank being examined offers merchant processing as an agent bank, refer to the agent bank procedures.

Overall objective: To assess the quantity and direction of risks in an acquiring bank's merchant processing activity; understand management's risk tolerance levels; gain an understanding of products offered or planned; assess policies, procedures, and practices used in merchant processing; and assess compliance with regulations and regulatory guidance.

This objective will be attained through completion of examination activities in some or all of the following functional areas.

Management Planning

Objective: To assess the adequacy of the strategic plan, business plan, and the overall planning process, including management's methodology for setting merchant processing growth and profitability targets, and the processes to ensure appropriate expertise and sufficient staffing within the line of business.

1. Review the bank's strategic plan and determine whether management's plans for the department are clear and represent the current direction of the department, as well as any changes since the last exam that may not be consistent with the bank's current strategic plan.

2. Determine whether the bank card associations have placed restrictive guidelines on the bank. If so, assess management's corrective action plan. Restrictions may include requiring a collateral pledge, maintaining higher levels of capital, or prohibiting the bank from signing certain types of merchants.

3. For issues that remain uncorrected, determine whether the board or its audit committee has adopted a corrective action plan and the status of implementing the corrective action plan.

4. Obtain, through discussion with the manager of the merchant processing department, information about the overall portfolio, MIS, and policies. Significant changes from the prior examination should be reviewed to understand how the changes have affected the portfolio's risk profile.

5. Evaluate any new programs the bank is pursuing and what effect the programs may have on the merchant operation.

6. Determine whether the bank has acquired any merchant portfolios since the previous examination. If so, determine

- thoroughness of the due diligence review performed by management before the purchase.
- quality of the portfolio as determined by the charge-back rate and loss history.
- number of accounts and breakdown of merchant accounts by industry (using standard industry code).
- whether reserve accounts or certificates of deposit are pledged against the merchant accounts.
- whether the purchase was approved by the board and management according to bank policy.

7. Determine the volume of transactions being processed in relation to the bank's tier 1 capital, in aggregate and for transactions deemed high risk.

8. Determine the risk profile of the portfolio. Evaluate the methods the bank uses to rate the risk in its merchant accounts, as well as the frequency and timing of adjusting the ratings of its merchant accounts.

9. Assess the adequacy of the overall MIS (information contained in MIS reports is detailed in the "Internal Control Questionnaire" in this booklet, under the "Management and Board Supervision" section, item 7). Review

   - MIS reports management routinely uses, and determine whether the reports adequately inform management of the department's condition.
   - reports to the board and determine whether the information the directors receive is meaningful and complete. At a minimum, reports should include information for each portfolio segment including agent bank and ISO/MSP portfolios. Information should include sales volumes, merchant types, profitability, charge-back activity, and fraud activity.

   Consider performing verification procedures if the reports and trial balances contain unusual information or information that cannot be readily explained.

10. Review the résumés of the principals in the merchant processing department. Determine whether the staff has adequate experience in merchant processing and is adequately trained.

11. Review the organizational chart for the department to determine what, if any, other responsibilities the merchant manager has within the bank. Determine whether the organizational structure is appropriate.

12. Determine what committees, if any, are involved in the merchant processing operation. Review the committee's minutes for pertinent information. Determine whether the committee structures, if any, are appropriate.
13. Determine whether current staffing levels fit the bank's short-term and long-term requirements. Determine whether

- staffing levels are adequate for the volume of merchant accounts, the number of applications reviewed daily, processing needs, and the need to oversee third parties.
- personnel reviewing merchant applications are qualified.
- staffing levels are sufficient to handle resolution of charge-backs within bank card association time frames.
- staffing levels are sufficient to investigate daily fraud exception reports in a timely manner.
- staff turnover is reasonable.

14. Determine whether there is a separate bank policy for merchant processing or whether it is incorporated within another bank policy, when the board approved the policy, and when the policy for merchant processing was last updated.

15. Evaluate the overall adequacy of written policies for merchant processing by considering whether the policy

    - establishes clear lines of authority and responsibility.
    - identifies the risks the bank is willing to accept, as well as limits on the amount of those risks in relation to capital, earnings, or sales volumes, as appropriate.
    - limits the individual and aggregate volume of the bank's merchant activity.
    - provides for adequate and knowledgeable staff.
    - requires written contracts between all third parties.
    - establishes criteria for the acceptance of merchants.
    - requires the development of procedures to monitor each merchant's activity.
    - establishes when merchant reserve (holdback) accounts are appropriate.
    - establishes risk-based guidelines for the periodic review of merchant creditworthiness.
    - develops criteria for contracting with any ISO/MSP to act as agent for the bank.
    - requires the development of adequate MIS to keep management and the board informed of the program's condition.
    - requires that a comprehensive procedures manual be developed to guide officers and employees in administering the program.
    - establishes guidelines for handling exceptions to policy.
    - establishes guidelines for the acceptance of agent banks.
    - requires review of all contracts and applications by legal counsel familiar with merchant processing.

16. Determine whether the board evaluates policies for changing market and business conditions at least annually and whether the policies are in line with the overall strategic plan for this activity.

17. Determine whether the bank policy addresses charging off stale charge-backs (generally 90 days) and assess the policy's appropriateness.

18. Determine whether the bank policy addresses the approval process for new merchant accounts. In that regard, and from an underwriting perspective, determine whether the policy addresses the following issues and points:

    - types of merchants for which the bank does not want to provide merchant processing services (prohibited and restricted lists).
    - documentation requirements for merchant files.
    - location of original contracts for merchants and requirement that they be maintained in a secure, fire-protected area.
    - merchant contracts have the appropriate party signatures.
    - underwriting guidelines for merchant accounts.
    - termination procedures for merchant accounts.
    - type of derogatory information that is acceptable on credit reports.
    - criteria for approving processing for additional merchant locations.
    - personnel in the bank who are responsible for approving merchants.
    - handling of exceptions to the merchant approval policy.
    - process for reviewing information collected by ISOs/MSPs.

19. Determine whether the board has adopted a policy for underwriting a new ISO/MSP. If so, determine whether the policy includes stipulations that

    - ISO/MSP must provide the acquiring bank certain financial information (the policy should stipulate its type and timing).
    - experienced commercial credit officer must review the periodic financial statements of the ISO/MSP.
    - management must review the depth and experience of the ISO/MSP management.
    - bank must perform required background checks, and the checks should determine whether any ISO/MSP or its principals have criminal records.
    - bank must obtain required bank and trade references on all ISOs/MSPs and their principals.
    - bank must identify whether the principals of the ISOs/MSPs are connected with the bank's directorate or management team and whether the ISOs/MSPs are related interests of the bank's directorate or management team.
    - ISO/MSP must maintain specific reserve accounts to absorb losses from merchant charge-backs or other damages if the organization is financially liable for losses.

20. Determine whether the acquirer has a policy that addresses agent banks for which the acquirer provides service. Does the policy address the following items?

    - Criteria for accepting agent banks.
    - Agent bank's merchant underwriting.
    - Policy exceptions.
    - Agent bank's liability.
    - Periodic reviews.

Underwriting and Card Sales

Objective: To determine whether sales and underwriting activity is consistent with business and strategic plans as well as risk tolerance objectives, and whether appropriate controls and systems are in place. To assess the quality of new merchants, identify any changes from past underwriting, determine the adequacy of and adherence to merchant processing policies and procedures, and gain a thorough understanding of the processes employed in underwriting and card sales activity.

1. Evaluate the bank's policy and process for approving new merchant accounts and determine whether it addresses the following issues and points:

    - Types of merchants for which the bank does not want to provide merchant processing services (prohibited and restricted lists, including OFAC's SDN List).
    - Documentation requirements for merchant files.
    - Location of original contracts for merchants and a requirement that these documents be maintained in a secure, fire-protected area.
    - Whether merchant contracts have the appropriate party signatures.
    - Underwriting guidelines for merchant accounts.
    - Termination procedures for merchant accounts.
    - Type of derogatory information that is acceptable on credit reports.
    - Criteria for approving processing for additional merchant locations.
    - Bank personnel responsible for approving merchants.
    - Handling of exceptions to the merchant approval policy.
    - Process for reviewing information collected by the ISO/MSP.

2. Evaluate the bank's procedures for ensuring compliance with the merchant approval policy.

3. Determine how the bank documents and monitors performance of exceptions to the merchant approval policy. Evaluate the practices for waiving documentation requirements.

4. Determine whether the bank has a written agreement with each merchant and whether the agreement contains the following information:

    - Fees to be charged to the merchant.
    - Requirements the merchant must meet at the point of sale.
    - Required information for charge-backs.
    - Merchant's redress if the agreement is terminated or suspended.
    - Whether the merchant must notify the bank of a change in ownership.
    - Whether the merchant is subject to continuing review by the bank or a designated third party.
    - Statement requiring the merchant to follow bank card association rules.

- Whether the merchant assumes liability for problems associated with unsecured transmission of card data and storage of customer information for Internet merchants.

5. Select a representative sample of recently approved merchant files (e.g., within the last 90 days). The sample should include merchants that the bank obtains directly, through ISOs/MSPs, and through agent banks. If possible, the sample of merchants obtained directly by the bank should include a sample of merchants by size and industry. Review the sample of merchant files for compliance with the policy.

6. Summarize the results of the merchant file review. Determine whether the level of exceptions is reasonable in view of board-approved policies.

7. In evaluating the bank's ongoing review of merchant accounts, determine the following:

   - Type or size of merchant accounts eligible for review.
   - Frequency of the review.
   - Whether the review is coordinated with the commercial loan department.
   - Type and timing of the financial information the bank asks merchants to provide.
   - Performance factors included in the review (e.g., level and trends in transactions, returns, and charge-backs).

8. Evaluate how the bank determines when to set up a merchant reserve or holdback. If reserves are established, how frequently are they reviewed?

Settlement and Charge-Backs

Objective: To evaluate the effectiveness of the settlement and charge-back function, including strategies and programs employed.

1. Review the settlement flow chart. Identify all parties involved, each party's responsibilities, and the estimated time that it takes funds and transaction data to flow from party to party during the settlement process.

2. If the bank does not pay merchants the same day it receives credit from issuers, assess management's procedures to keep the funds segregated and liquid.

3. Review management's analysis of risk if the bank uses a BIN/ICA number (whether the bank owns the number or not).

4. Check with the examiner reviewing the bank merchant processing policy and confirm that the policy addresses charging off stale charge-backs (generally 90 days) and the appropriateness of the policy. If different examiners are handling assignments regarding policy review and charge-back review, be sure both examiners agree on the dynamics of the bank's policy regarding charge-offs.

5. Review the trend in the volume and aging of charge-backs.

6. Investigate significant trends in both the volume and age of charge-backs. Consider

   - discussing with management any merchants that are generating significant charge-backs.
   - instructing the bank to charge off any charge-backs aged over 90 days (bank card association rules allow exceeding 90 days in limited circumstances).
   - whether the bank has suffered any significant losses from merchant charge-backs over the past several years.

7. Evaluate the adequacy of the charge-back system. Determine whether the system is automated or manual and whether it can

   - quantify outstanding charge-backs and their ages.
   - prioritize research into charge-backs.
   - measure the efficiency of the charge-back process.

8. Determine how the bank evaluates the adequacy of its charge-back systems.

9. Determine how the bank plans for contingencies, such as large merchant bankruptcies, which can generate a large volume of charge-backs.

10. Describe how management assigns charge-back work to employees, such as by age, reason code, or merchant.

11. Review the bank's procedures for establishing merchant-funded charge-back reserves on high-charge-back merchants. Determine whether current practices sufficiently protect the bank from exposure to charge-back loss.

12. If the bank is not adequately protected from charge-back losses, determine whether the bank needs a bank-funded general reserve or additional capital support.

13. Evaluate the collection of charge-back losses and uncollected fees.

Profitability

Objective: To assess the quantity, quality, and sustainability of earnings from merchant processing activities.

1. Review the merchant processing department's profitability statements. Evaluate major costs and fee income items in relation to overall profitability. Determine the impact of charge-back and fraud losses on profitability.

2. Identify whether the merchant processing department generates a profit or loss and the amount from the prior year-end and current YTD.

3. If the merchant processing department is unprofitable, determine the bank's appetite, plan, and rationale for continuing the operation.

4. Review the bank's budgeting process for its merchant processing department and investigate the budget's significant variances from actual performance. Determine whether the department is expected to meet this year's budget and, if not, why not.

5. Evaluate the MIS used in determining the department's profitability.

6. Determine how management arrives at cost figures, i.e., whether it uses actual or estimated costs, and whether the methodology is appropriate.

7. Review the bank's pricing policies and evaluate the bank's pricing methods. If the bank offers reduced discount rates based on other existing banking relationships, evaluate the risks and rewards.

8. Review management's analysis of whether individual merchants are profitable for the bank. Investigate reasons for low profitability or losses.

9. Obtain discount rates from the merchant file review worksheet and compare actual pricing against the pricing policy.

10. Determine which personnel have the authority to set pricing variables and how management monitors the pricing process.

11. Coordinate with the examiner reviewing third-party organizations to determine other pricing programs used. Determine whether pricing is tied to the sale or lease of equipment or other services.

Risk Management and Control Systems

Objective: To assess adequacy of the bank's processes for identifying, measuring, monitoring, and controlling risk by reviewing the effectiveness of risk management and other control functions.

1. Determine the internal/external auditor's knowledge of the merchant processing department and whether the auditor's knowledge is adequate to perform effective reviews.

2. Review the scope and frequency of the internal audit. Determine whether it addresses all operational areas.

3. Determine whether internal audit reviewed the bank's merchant processing activity or operation. If a review was conducted, look at the latest findings of the review by internal audit, bank management's response to the review findings, and the status of addressing any corrective actions for the findings.

4. Determine whether internal audit reviews major services provided by third-party organizations.

5. Confirm whether external audit reviewed the bank's merchant processing activities. If a review was conducted, look at the latest findings of the review by external audit, bank management's response to the review findings, and the status of addressing any corrective actions for the findings.

6. Determine whether the scope and frequency of fraud reviews are adequate. Assess how analysts prioritize exceptions and whether certain potentially suspicious transactions are processed through more sophisticated systems (e.g., scoring and other databases).

7. Determine whether management has established parameters for monitoring Internet transactions.

8. Determine how the bank establishes parameters for exceptions.

9. Determine who in the bank can set fraud parameters and what documentation is required to change the parameters.

10. Determine the frequency with which management updates a merchant's historical sales volume.

11. Determine the bank's course of action when it detects suspicious activity. (Does the bank delay settlement, establish merchant-funded reserves, or file a SAR, for example?)

12. Review the acquiring bank's controls over delaying settlement funds to determine whether they comply with bank card association rules.

13. Review any parameters for exceptions that are available to the acquirer but not presently in use. Commonly used parameters are:

    - Large average ticket size.
    - Large daily or weekly volume.
    - Keyed rather than swiped transactions.
    - Multiple tickets in the same dollar amount.
    - Multiple uses of same cardholder number.
    - High charge-back activity.
    - Excessive return volumes.
    - Declined authorizations.
    - Authorizations not matched to sales and vice versa.
    - Transactions from inactive or closed accounts.

14. If a neural network is used, review management's rationale for the parameters that have been set.

15. Assess the adequacy of the overall MIS (information contained in MIS reports is detailed in the "Internal Control Questionnaire" in this booklet, under the "Management and Board Supervision" section, item 7).

    - Review the MIS reports routinely used by management and determine whether the reports adequately inform management of the department's condition.
    - Review reports to the board and determine whether the information the directors receive is meaningful and complete. At a minimum, reports should include information for each portfolio segment, including agent bank and ISO/MSP portfolios. Information should include sales volumes, merchant types, profitability, charge-back activity, and fraud activity.

    Consider performing verification procedures if the reports and trial balances contain unusual information or information that cannot be readily explained.

Third-Party Vendor Management and Agent Banks

Objective: To determine the extent of all third-party arrangements in merchant processing, including agent bank arrangements, and evaluate the effectiveness of management's oversight and risk management processes.

1. Determine what third-party organizations the acquiring bank uses for merchant processing services and the activities or services the third party performs.

2. Obtain a report that shows merchant sales volume for each ISO/MSP. Review ISOs/MSPs that have significant volume or growth.

3. Determine whether contracts are on file for each third-party organization.

4. Evaluate whether the bank periodically reviews its third-party organizations and, if so, the frequency of the reviews. Information available may include financial statements, third-party operational reviews, disaster contingency plans, and bank regulatory agency reports.

5. Review major contracts to assess the following information:

    - Terms specifying financial compensation, payment arrangements, and price changes.
    - Provisions prohibiting the third party from assigning the agreement to any other party.
    - Frequency and means of communication and monitoring activities of each party.
    - Specific work to be performed by the third-party servicer.
    - Requirements for the confidential treatment of records.
    - Record-keeping requirements each party must adhere to and whether the other party has access to these records.
    - Responsibility for audits and whether the acquirer has the right to audit the third-party organization.

- Notification requirements of system changes that could affect procedures and reports.
- Type and frequency of financial information the third party will provide.
- Whether contractual penalties for terminating the contract seem reasonable.

6. Review a sample of ISO/MSP contracts for the appropriate provisions. In addition to general contract provisions, the contracts should

   - tie fees to performance and adherence to contract terms (e.g., number and quality of merchants, volume of sales transactions, or charge-back activity).
   - define responsibilities for fraud and charge-back losses.
   - require security deposits from the ISO/MSP if its financial condition is weak or the quality of the merchants it solicits on behalf of the bank is poor.
   - include remedies to protect the bank if the ISO/MSP fails to perform (including indemnity, early termination rights, and delayed payment of residuals).
   - state the criteria for accepting merchants.
   - specify that the bank owns the merchant relationships.
   - control the future use and solicitation of merchants.
   - define the allowable use of the bank's and the ISO's/MSP's name, trade name, and logo.
   - permit bank employees to conduct on-site inspections of the ISO/MSP.
   - warrant that all federal consumer laws and bank card association rules are to be followed.

7. Review a sample of ISO/MSP credit files and check for compliance with policy. At a minimum, the files should contain

   - analysis of the current financial statements of the principals of the ISO/MSP. The type of financial statement should correlate to the size of the company.
   - document detailing a bank employee's on-site inspection of the ISO/MSP.
   - evidence that bank and trade references have been verified.
   - credit report on the principals of the ISO/MSP.
   - criminal check on the principals of the ISO/MSP.
   - disclosure of and details concerning any connections or related interest between the bank directorate or management and the ISO/MSP or its principals.

8. Determine whether ISO/MSP reserve accounts are consistent with the condition of the company and the volume of business generated.

9. Determine the frequency of the bank review of the ISO/MSP reserve accounts, how often the reserve balances can be changed, and the process for increasing or decreasing the reserve balances, as well as the approval process.

10. List third-party processors that have provided contingency plan information to the bank. Review the bank's analysis of contingency plans to determine adequacy. If an analysis does not exist, review the reasonableness of contingency plans.

11. Determine whether third-party contingency plans are adequately considered in the bank's overall contingency plan.

12. Review the merchant processing department's procedures for monitoring the third party's quality control and compliance with the contract. Monitoring for quality control should (as applicable)

    - ensure that the ISO/MSP is properly registered with the bank card associations.
    - determine the adequacy of the ISO/MSP's written operating procedures.
    - ensure that the bank approves all ISO/MSP training materials, marketing materials, and discount and fee schedules.
    - verify that ISO/MSP sales personnel meet the bank's criteria for criminal background and credit checks.
    - sample merchants solicited by the ISO/MSP for compliance with the bank's policies.
    - compare approval and rejection rates with department projections.
    - review the quality of customer service activities.
    - review how the bank and the ISO/MSP resolve merchant complaints.
    - evaluate the timeliness of charge-back processing and appropriateness of decisions.
    - evaluate how decisions were made on exceptions that could affect fraud monitoring.
    - determine the adequacy of merchant and third-party reserve accounts, if appropriate.
    - assess compliance with bank card association regulations.

13. Determine whether the management of the merchant department requires the third party to adopt a written action plan to correct deficiencies when results fall below bank standards.

14. Review the bank's MIS used to monitor ISO/MSP activities.

15. Determine the monitoring levels and reasonableness of ISO/MSP system access. All system changes should have prior approval of a bank employee.

16. Review the bank's agent bank programs and determine the level of liability assumed by the acquirer.

17. Determine where agent bank contracts are kept and whether they are in a secure and fire-protected area.

18. Determine whether agent bank contracts contain the appropriate party signatures.

19. Obtain a report that shows merchant volume per agent bank. Review agent banks that have a significant volume of transactions.

20. Review a sample of agent bank files. Evaluate whether the information in the files is adequate and check for compliance with policy.

Complete the internal control questionnaire, if needed, to further assess the adequacy of the bank's internal controls. Otherwise, refer to the procedures in the "Conclusions" section.

Agent Banks

These examination procedures apply to agent banks. If the bank being examined offers merchant processing as an acquiring bank, refer to the acquiring bank procedures.

Overall objective: To assess the quantity and direction of risks in an institution's merchant processing activity; understand management's risk tolerance levels; gain an understanding of products offered or planned; assess policies, procedures, and practices used in merchant processing; and assess compliance with regulations and regulatory guidance.

This objective will be attained through completion of examination activities in some or all of the following functional areas:

Management Planning

Objective: To assess the adequacy of the strategic plan, business plan, and the overall planning process, including management's methodology for setting merchant processing growth and profitability targets, and the processes to ensure appropriate expertise and sufficient staffing within the line of business.

1. Determine management's understanding of merchant processing activities (i.e., ability to understand liability and responsibilities under the agent bank agreement).

Underwriting and Credit Card Sales

Objective: To determine whether sales and underwriting activity is consistent with business and strategic plans as well as risk tolerance objectives, and whether appropriate controls and systems are in place. To assess the quality of new merchants, identify any changes from past underwriting, determine the adequacy of and adherence to merchant processing policies and procedures, and gain a thorough understanding of the processes employed in merchant processing underwriting and merchant processing credit card sales activity.

1. For agent banks that retain loss liability, document the volume of merchant transactions the agent bank has processed for the prior year and YTD.

2. For agent banks that retain loss liability, determine the source and composition of the bank's merchant portfolio.

3. For agent banks that retain loss liability, determine whether the bank performs its own underwriting. If so, review a sample of new merchant accounts to determine compliance with underwriting standards.

4. If the bank has a significant volume of merchant processing activity in relation to its capital base, determine whether the bank has adequate policies in place to control risks. Determine whether the policy

- addresses underwriting standards (customers vs. noncustomers), pricing, liability provisions, and management and board reporting.
- states who is authorized to approve merchants and outlines procedures for approving exceptions.

Settlement and Charge-Backs

Objective: To evaluate the effectiveness of the settlement and charge-back function, including strategies and programs employed.

1. Determine types and adequacy of information on merchant charge-backs and on the bank's monitoring for fraud.

2. For agent banks that retain loss liability, determine whether the bank maintains any merchant holdback reserves to mitigate risk.

3. For agent banks that retain loss liability, determine whether the bank has incurred any significant charge-back or fraud losses in the past year.

4. For agent banks that retain loss liability, determine whether the acquiring bank or the agent bank shares a BIN/ICA number with other banks. If so, determine who is responsible for fraud and charge-back losses experienced by any other bank processing under the BIN/ICA number. More specifically, determine who is contractually responsible for what (e.g., fraud, charge-backs) based on contracts between parties. Also, determine whether the bank has taken any higher risk posed by contractual relationships into account for capital and planning purposes.

Profitability

Objective: To assess the quantity, quality, and sustainability of earnings from merchant processing activities.

1. For agent banks that retain loss liability and if the bank sets pricing variables, determine what pricing variable method is used (e.g., matrix, formula, or pricing model). Consider whether

   - pricing system takes into account all of the bank's costs.
   - pricing on the bank's largest merchant accounts (e.g., top 10) is profitable.

2. For agent banks that retain loss liability, analyze profitability by reviewing income statements and profitability reports on the bank's merchant activity.

3. Determine who has the authority to price a merchant account outside the pricing guidelines. Select a sample of merchant accounts to determine whether exceptions were properly approved.

Risk Management and Control Systems

Objective: To assess adequacy of the bank's processes for identifying, measuring, monitoring, and controlling risk by reviewing the effectiveness of risk management and other control functions.

1. Determine the adequacy of the agent bank's systems for monitoring the credit risk of its largest merchants. Determine whether the agent relies on the acquiring bank to conduct periodic reviews.

2. For agent banks with loss liability, determine whether the merchant portfolio has concentration risk by industry, merchant segment, or individual merchant that could adversely affect the bank.

3. Determine whether the board has established policies on concentration limits in relation to bank capital, earnings, or sales volumes as appropriate.

4. Assess whether adequate controls are in place to identify and measure the bank's risk (e.g., reporting and portfolio analysis).

5. Evaluate the internal audit program to ensure that its reviews are commensurate with the volume and quantity of risk in the program.

Third-Party Vendor Management and Agent Banks

Objective: To determine the extent of all third-party arrangements in merchant processing, including agent bank arrangements, and evaluate the effectiveness of management's oversight and risk management processes.

1. Obtain all agent bank agreements/arrangements and review to ensure that they

   - are current and in writing.
   - define the party responsible for fraud and charge-back losses.
   - identify who is responsible for underwriting new merchants.
   - identify who will price the merchant account.
   - specify the income the agent will receive.
   - contain confidentiality provisions.
   - define the sharing of BIN/ICA number, if applicable.

2. By reviewing the agent bank agreements, determine whether the bank is acting only as a referral bank and has no liability for fraud and/or charge-back losses.

3. For agent banks with liability obtain the following information. This information is used to address other functional areas and other procedures regarding banks that retain loss liability.

- Monthly volume and profitability reports from the acquiring bank.
- Reports on monitoring charge-backs and fraud.
- Merchant processing policies.

4. Determine whether the referral/agent bank has signed any indemnification agreements on individual merchant accounts that the acquiring bank would have otherwise denied. If not, no further work is recommended for referral banks. If so, review a sample of these accounts to determine whether the referral bank took on excessive risk in signing these merchants.

5. Assess the adequacy of customer support provided to the agent by the acquirer under the terms of the agent bank agreement. For example, determine whether customer support includes the following services:

   - Periodic management reports on portfolio volume and activity.
   - Notification of charge-back volumes and actual losses from charge-backs and fraud.
   - An annual risk profile.
   - Training.

Conclusions

Conclusion: The aggregate level of each associated risk is (low, moderate, or high).
The direction of each associated risk is (increasing, stable, or decreasing).

This section applies to acquiring banks and agent banks.

Objective: To determine, document, and communicate overall findings and conclusions regarding the examination of merchant processing.

1. Determine preliminary examination findings and conclusions and discuss with the EIC, including

   - quantity of associated risks (as noted in the "Introduction" section).
   - quality of risk management.
   - aggregate level and direction of associated risks.
   - overall risk in merchant processing.
   - violations and other concerns.

Summary of Risks Associated With Merchant Processing				
Risk category	**Quantity of risk** (Low, moderate, high)	**Quality of risk management** (Weak, satisfactory, strong)	**Aggregate level of risk** (Low, moderate, high)	**Direction of risk** (Increasing, stable, decreasing)
Credit				
Operational				
Compliance				
Strategic				
Reputation				

2. If substantive safety and soundness concerns remain unresolved that may have a material adverse effect on the bank, further expand the scope of the examination by completing verification procedures.

3. Discuss examination findings with bank management, including violations, recommendations, and conclusions about risks and risk management practices. If necessary, obtain commitments for corrective action.

4. Compose conclusion comments, highlighting any issues that should be included in the report of examination. If necessary, compose an MRA comment.

5. Update the OCC's information system and any applicable report of examination schedules or tables.

6. Write a memorandum specifically setting out what the OCC should do in the future to effectively supervise merchant processing in the bank, including time periods, staffing, and workdays required.

7. Update, organize, and reference work papers in accordance with OCC policy.

8. Ensure any paper or electronic media that contain sensitive bank or customer information are appropriately disposed of or secured.

Internal Control Questionnaire

An internal control questionnaire (ICQ) helps an examiner assess a bank's internal controls for an area. ICQs typically address standard controls that provide day-to-day protection of bank assets and financial records. The examiner decides the extent to which it is necessary to complete or update ICQs during examination planning or after reviewing the findings and conclusions of the core assessment.

Policies and Procedures

1. Has the board adopted a written policy on merchant processing that

    - establishes clear lines of authority and responsibility?
    - identifies the risks the bank is willing to accept, as well as limits on the amount of those risks in relation to capital, earnings, or sales volumes, as appropriate?
    - limits the individual and aggregate volume of the bank's merchant processing activity in relation to capital, earnings, or sales volumes, as appropriate?
    - provides for adequate and knowledgeable staff?
    - requires written contracts between all third-party organizations?
    - establishes criteria for the acceptance of merchants?
    - requires the development of procedures to monitor the activity of each merchant?
    - establishes when merchant reserve (holdback) accounts are appropriate?
    - establishes risk-based guidelines for the periodic review of merchant creditworthiness?
    - develops criteria for contracting with an ISO/MSP to act as agent for the bank?
    - requires the development of adequate MIS to keep management and the board informed of the program's condition?
    - requires an annual analysis of capital adequacy and allocation of capital in relation to the merchant processing risk profile and volumes?
    - requires that a comprehensive procedures manual be developed to guide officers and employees in administering the program?
    - establishes guidelines for handling exceptions to policy?
    - establishes guidelines for the acceptance of agent banks?
    - requires review of all contracts and applications by legal counsel familiar with merchant processing?

2. Are merchant processing policies and objectives reviewed at least annually to determine their compatibility with current market conditions and the bank's strategic plan?

3. Is the procedures manual comprehensive and current and does it provide for

    - establishing new business?
    - monitoring existing business?
    - dealing with ISOs/MSPs?
    - handling complaints with merchants?

- conducting settlement procedures—both ACH and wire transfer?
- processing merchant retrievals and charge-backs?
- addressing fraud monitoring and reporting?
- training new personnel?

Management and Board Supervision

1. Does the merchant processing department have an organizational chart?

2. Does the manager of the merchant processing operations have merchant processing experience?

3. Are the reports received by the board and management appropriate and timely?

4. Have appropriate backup managers and staff been trained to handle critical areas?

5. Does the staffing keep pace with the volume of merchant applications received daily?

6. Is staff turnover reasonable?

7. Do MIS reports include information on

   - concentrations by type of industry in relation to sales volumes and bank capital?
   - geographic distribution of merchants?
   - high-volume merchants in relation to sales volumes and bank capital?
   - attrition?
   - number of active merchant accounts?
   - aggregate sales volume for the month and year?
   - number of transactions for the month and year?
   - average discount rate of the portfolio?
   - average per unit cost?
   - whether the bank profits from each merchant? (The report should show which merchants are not profitable for the bank.)
   - charge-backs as a percentage of sales?
   - new merchants?
   - audit-deficiency tracking?

8. Has the board adopted a strategic plan for the department?

9. Is the board adequately informed about merchant processing activities?

10. Is a separate pro forma budget prepared for the department? Does it include an analysis of capital allocated relative to the risk profile of the merchant processing activity?

11. Has the board reviewed the department's bonding needs?

12. Does the bank have an effective project management function to ensure timely implementation of new products and systems?

13. Do the personnel reviewing funding needs for the bank consider the impact of merchant processing?

Audit Coverage

1. Does the merchant processing department receive audit coverage?

2. Is the internal/external auditor knowledgeable about merchant processing?

3. Do audit reports, for both the bank and third parties, require written management responses to significant deficiencies?

4. Do merchant processing audits

   - address all operational areas?
   - verify that the board has approved risk limits, such as processing volume, types of merchants, geographic restrictions, and concentrations by industry and large merchants in relation to capital, earnings, and sales volumes, as appropriate?
   - test compliance with policy?
   - determine compliance with departmental operating procedures?
   - ensure that the department has adequate processes to comply with bank card association rules?
   - assess compliance with written contracts?
   - test adherence to approval authorities delegated to department employees?
   - verify that the bank's contingency planning coordinator periodically reviews the adequacy of each third party's disaster recovery plan?
   - validate the accuracy of cost accounting controls in determining the effectiveness of pricing and profitability analyses?
   - ensure that changes in discount rates and fees are authorized by management?
   - ensure that departmental staff periodically review third-party deposit accounts for unusual activity?
   - validate the accuracy and controls involved for the bank's merchant and ISO/MSP reserves?
   - determine the appropriate usage and reconciliation of balance sheet accounts?
   - determine that management appropriately accounts for stale balance sheet items in balance sheet accounts?
   - assess overall risk in the area?

5. Does the bank require that all ISOs/MSPs have operational audits?

Approving Merchants

1. Does the policy on approving merchants provide for clear and measurable underwriting standards for merchants?

2. Does the bank require merchant applications to be in writing?

3. Does the bank perform inspections or use other types of verifications for all merchants?

4. Are the inspections and verifications documented?

5. Are statements of previous merchant activity required for all new merchant applications?

6. Does the policy address

   - desirable vs. undesirable merchants?
   - documentation requirements for each merchant's file?
   - who is authorized to approve merchants?
   - merchant underwriting guidelines?
   - merchant termination procedures?
   - handling exceptions to the merchant approval policy?
   - type and timing of financial information to be provided by merchants?

7. Does the person reviewing merchant applications have credit experience?

8. Are the financial statements of all large merchants reviewed by a person (or committee) with extensive commercial loan experience?

9. Are the financial statements of all large merchants reviewed at least annually?

10. Does the bank require reserves against the accounts of high-risk merchants or those of merchants incurring a significant amount of charge-backs?

11. Are merchant reserve accounts kept separate from their operating accounts and not commingled with other merchant reserve accounts?

Settlement Process

1. If processing failure occurs at any point, is the bank obligated to fund merchant sales?

2. Does the bank settle directly with the merchant?

3. Are written agreements in place for parties involved in the settlement process?

4. Are contracts with network vendors made with the acquirer rather than ISOs/MSPs?

5. Are all merchant and ISO/MSP funds held as charge-back or loss reserves placed in individual deposit accounts, separate from settlement proceeds?

6. Is access to merchant and ISO/MSP reserve accounts restricted to bank personnel?

7. Are adequate procedures followed to refund merchant and ISO/MSP reserves according to the terms in the merchant agreement?

8. When merchant reserves cannot be successfully refunded, do procedures ensure compliance with abandoned property and state escheat laws?

9. Can the bank hold merchant funds pending the resolution of suspected fraudulent or sanctioned activity?

10. Are payments to merchants made with collected settlement funds (funds for sales received from the issuer via the associations)?

11. Are merchant and ISO/MSP accounts reviewed for suspicious activity?

12. Have contingency plans been developed and reviewed for all parties involved in the settlement process?

13. If ISO/MSPs perform accounting and servicing functions, have contingency plans been developed to cover their services?

14. Are there procedures to ensure the accuracy of ACH and wire transfer files, whether originated at the bank or by a third-party processor?

15. Are there controls for handling rejected ACH and wire transfer items?

16. Has the bank ever missed any settlement cutoff times with any counterparty?

17. Which merchants are settled by wire versus ACH?

18. Has management obtained third-party reviews and regulatory examination reports of its processors?

Charge-Back Processing

1. Are policies and procedures in place for charge-back processing?

2. Can the bank generate reports on

   - daily charge-back activity?
   - status and aging of charge-backs?
   - exception reports on merchants experiencing unusual charge-back activity?

3. Are losses from merchant charge-backs clearly identified on the general ledger as noninterest expense?

4. Does the bank debit merchants for charge-back at the same time the bank pays the issuer?

5. Is the staff sufficient to process retrieval requests and charge-backs within the bank card association's time frames?

Fraud Detection

1. Does the bank have an early warning system to detect merchant fraud?

2. Are fraud reports reviewed daily?

3. Are bank employees trained in detecting merchant fraud?

4. Are exception parameters for fraud reports tailored to each merchant?

5. Do exception reports screen for

   - significant variances from average ticket size?
   - significant variances in daily and weekly volume?
   - multiple tickets in the same dollar amount?
   - multiple uses of same cardholder number?
   - keyed rather than swiped transactions?
   - transactions from inactive or closed accounts?
   - high rate of charge-backs?
   - authorizations not matched to sales, and vice versa?
   - authorization declines?
   - excessive returns relative to sales?

6. Does the bank have a process for filing SARs with FinCEN in accordance with 12 CFR 21.11 for national banks or 12 CFR 163.180 for FSAs, as applicable?

7. Does management have an effective process to respond to bank card association reports in a timely manner?

8. Are fraud losses reported on the call report as noninterest expenses?

9. Does management perform postmortem analyses of fraud losses?

Agent Banks

1. Are agent bank agreements in writing?

2. Are agent banks informed of their financial liability for a merchant's fraud and charge-back losses?

3. Are merchants obtained through agent banks subject to the same underwriting standards as direct or ISO/MSP merchants?

4. Does the bank routinely obtain and review financial information on agent banks?

5. Are separate files maintained for each agent bank?

6. Are proper approval authorities obtained for each agent bank?

7. Does the policy on selecting agent banks address

   - bank's financial condition?
   - early termination of the relationship with the agent bank if unsafe and unsound activities are suspected?
   - periodic financial review of agent banks with high-volume or high-risk merchants?

Third-Party Organizations

1. Has the bank registered all ISOs/MSPs with bank card associations?

2. Does the bank periodically analyze or review the finances of all third-party organizations?

3. Does the bank perform periodic on-site inspections of all bank ISOs/MSPs?

4. Does the bank review and approve all promotional materials used by ISOs/MSPs?

5. Does the bank attend sales training sessions for ISO/MSP salespeople?

6. Does the bank require that each ISO/MSP have operational audits?

Pricing

1. Does the bank's pricing policy address

   - minimum discount rates?
   - pricing methods used, such as standard matrix or bid models?
   - handling exceptions to the pricing policy?
   - which personnel, including ISO/MSP salespeople, have the authority to price merchants?
   - monitoring whether merchants are profitable for the bank?
   - repricing guidelines?
   - documentation requirements for discount rate reviews?

2. Does the bank's pricing system address:

    - overhead costs, including employee costs, educational and training costs, and occupancy costs?
    - internal and external processing costs, including cost of computer hardware, software, and phone lines?
    - interchange fees?
    - bank card association assessments?
    - revenue for providing float to the clearing process?
    - charge-back costs?
    - desired profit margins?
    - insurance and bonding needs?
    - loss history and the risk of future loss?

3. Does the bank track the date the merchants were last repriced?

4. Does the bank ensure that all outlets related to a merchant account are priced consistently?

5. Can the bank determine whether individual merchants are profitable for the bank?

Department Profitability

1. Does the department have a separate financial statement from the other areas in the bank?

2. Does the merchant department's profitability statement include all direct and overhead costs, including corporate allocations?

3. Does the department have an approved budget, and, if so, does the budget seem realistic?

4. Are significant variances from the budget explained?

5. Does the MIS provide information regarding the following?

    - Sales volume.
    - Total transactions.
    - Return on sales.
    - Per transaction/unit cost.
    - Per transaction/unit income.
    - Overhead per merchant.
    - Attrition rates.
    - Unprofitable merchants.

Card Equipment

1. For those banks providing point-of-sale equipment to merchants, is access to the inventory limited to authorized personnel?

2. Are inventory control logs maintained?

Conclusion

1. Is the foregoing information considered an adequate basis for evaluating internal control in that there are no significant additional internal auditing procedures, accounting controls, administrative controls, or other circumstances that impair any controls or mitigate any weaknesses indicated through the steps in this section (explain negative answers briefly and indicate conclusions as to their effect on specific examination or verification procedures)?

2. Based on the answers to the foregoing questions, internal control for merchant processing is considered (strong, satisfactory, or weak).

Verification Procedures

Verification procedures are used to verify the existence of assets and liabilities, or test the reliability of financial records. Examiners generally do not perform verification procedures as part of a typical examination. Rather, verification procedures are performed when substantive safety and soundness concerns are identified that are not mitigated by the bank's risk management systems and internal controls.

1. Test the additions to the trial balance(s) and the reconciliation of the trial balance(s) to the controlling subsidiary ledger(s).

2. Using an appropriate sampling technique, select merchants from the reports and

   - prepare and mail confirmation forms to merchants (confirm sales volumes as of last statement date).
   - after a reasonable period of time, mail second requests.
   - follow up on any failures to reply or exceptions and resolve differences.

3. Using the sample from item 2, review merchant files and

   - examine each merchant agreement for completeness and appropriate approval authority.
   - if the agreement requires holdbacks or reserves, compare actual on-deposit holdings against required levels; investigate discrepancies.
   - check the current discount rate and ensure that it complies with the pricing policy in place at time of approval or repricing.
   - check application estimates for volume and average ticket size to determine how much they vary from actual performance.
   - check to determine whether management ran the merchant against MATCH and OFAC's SDN List.

4. Obtain or prepare a schedule showing monthly transaction volume, monthly charge-back volume, and all associated monthly revenues and expenses since the last examination, then do the following:

   - Investigate all significant fluctuations or trends.
   - Determine whether the transaction volumes and charge-back volumes are commensurate with the revenues and expenses.
   - Trace revenue and expense transactions to source documents if unusual variances exist.

Appendixes

Appendix A: Portfolio Profile Worksheet

This worksheet is provided for informational purposes, but it is typically no longer used, because much of this information is now provided through various MIS reports provided by the institutions.

Bank name	
Bank address	
Type of merchant processing activity (acquirer or agent, with or without risk)	
Name of merchant processing contact person	
Phone number of contact person	
Bank Internet address	
Number of employees dedicated to merchant processing activities	#
Number of Visa BINs owned/active	#
Number of MasterCard ICAs owned/active	#
Are any BINs/ICAs shared with another bank? (yes or no)	
Sales volumes processed	
YTD (/ /)	$
YE prior year 1	$
YE prior year 2	$
Number of transactions—YTD and prior year	#
Average ticket size—YTD and prior year	$
Total number of merchants	#
Number of active merchants	#
Internet sales volume processed	$
Geographic concentration (local, regional, national)	
Three largest merchants by sales volume (include name and YTD sales volume)	1.
	2.
	3.
Current attrition level	%
Niche market (if applicable)	

Processing systems	
Front-end authorization and capture (major front-end systems used)	
Back-end processing system (in-house or vendor name)	
Charge-backs	
Charge-back monitoring system (in-house or vendor name)	
Charge-backs processed—YTD	$
Charge-backs processed—YE prior year 1	$
Charge-backs processed—YE prior year 2	$
Charge-back ratio (dollars)—YTD	%
Charge-back ratio (number)—YTD	%
Fraud monitoring	
Fraud monitoring system used (in-house or vendor name)	
Gross fraud losses—YTD	$
Net fraud losses after reimbursement/indemnification	$
Gross fraud losses—YE prior year 1	$
Net fraud losses after reimbursement/indemnification	$
Gross fraud losses YE prior year 2	$
Net fraud losses after reimbursement/indemnification	$
Reserve volumes	
General merchant reserves	$
Specific merchant reserves	$
ISO/MSP reserves	$
ALLL merchant reserves	$

Profitability information	
Typical retail discount	%
Typical retail per-item charge	$
Typical application fee	$
Typical statement fee	$
Typical charge-back fee	$
Equipment sales (in-house or vendor name)	
Independent sales organizations	
Number of ISOs used	#
Association information	
Visa sales processed (%)	%
MasterCard sales processed (%)	%
Total pledged to Visa, if applicable (dollars)	$
Total pledged to MasterCard, if applicable (dollars)	$
Is the bank in the Visa High-Risk Acquirer Program? (yes or no)	

Appendix B: Request Letter

Merchant Processing Request Letter Enclosure

Please provide copies of the following:

Management and Board Supervision

1. Current organizational chart for the department.
2. Résumés for all principals in the department.
3. Job descriptions for all principal positions.
4. Strategic and business plans and budgets for the department.
5. Management's annual analysis of capital adequacy and capital allocation relative to the risk profile of merchant processing activities.
6. Two most recent sets of monthly management reports routinely reviewed by management and the board.
7. Report on new merchants or management summaries for the previous three months.
8. Report on any credit risk management reports of merchant accounts.
9. Report on the bank's top 50 merchants by volume.
10. Report on the bank's merchants that are currently identified as highly suspect merchants by volume.
11. Concentration reports by industry code and state or geographic area.

Sales

12. Brief explanation of sales/account acquisition channels.

Underwriting

13. List of all insider-related merchant customers.
14. Samples of merchant agreements and applications.
15. List of all merchant reserves.

Profitability

16. Profitability report for the merchant processing department for the most recent year-end and year-to-date.

17. Current fee schedule and definitions of fees charged. If a particular fee includes various components, identify what items are included in the specific fee.

18. Profitability reports by sales segment.

19. An analysis of whether the bank's merchants are profitable for the bank, if available.

20. Report detailing total number of merchants, annual volume of sales, and number of transactions.

21. Listing of the unprofitable accounts.

22. Attrition report for the past year.

Agent Banks

23. Brief summary of the agent bank programs offered.

24. Name and address of agent banks, and the volume of merchant processing by these banks.

25. Sample agent bank agreement.

Third-Party Organizations

26. List of third parties used by name and address and description of service provided. Are any of the third-party arrangements new to the bank within the last 12 months? If so, please provide an electronic copy of the contract agreement in place with the third party.

27. Names and addresses of each ISO/MSP, and number of merchants, sales volume, and number of transactions attributable to each ISO/MSP.

28. List of any loan relationships to third parties, including loan terms and amounts.

29. Most recent bank audit report of ISO/MSP activity and ISO/MSP response.

30. Summary of which ISO/MSP has access to the acquirer's data-processing system and the extent of the access (e.g., set-up, charge-backs, or maintenance).

31. List of all ISO/MSP reserves and applicable balances.

Settlement

32. A flow chart and brief explanation of the settlement process that illustrates the parties involved and the timing of settlement.

Risk Management

33. Management summary of underwriting exceptions/overrides.

34. Brief description of the fraud monitoring process, the systems and reports used, prioritization of investigations, and staffing involved in the process.

35. Examples of daily fraud monitoring reports.

36. Parameter setting summary for fraud monitoring system.

37. Brief description of the charge-back process, the systems and reports used, prioritization of the research process, and staffing involved in the process.

38. Charge-back aging report, charge-back ratios, and trend analysis.

39. Fraud loss history for the most recent year-end and year-to-date. Were SARs filed for the fraud losses identified?

40. Credit loss history for the most recent year-end and year-to-date.

41. The last four quarterly monitoring reports for each association (Visa, MasterCard, and any others).

42. Any additional risk analysis or reports used to evaluate the portfolio apart from daily monitoring reports.

Audit

43. Most recent internal/external audit reports and management's response.

Portfolio Acquisitions

44. Listing of any portfolio acquisitions in the past 24 months.

45. Due diligence process used for portfolio acquisitions.

46. Management reports used to monitor and manage acquired portfolios.

Loan Review

47. Copies of internal loan review and loan review reports for the merchant processing activity, because the merchant processing business involves the fundamental evaluation of counterparty credit risk with significant merchants, ISOs/MSPs, and Rent-a-BIN partners. Also, provide any management responses for internal loan review reports.

Please make the following available upon our arrival at the bank:

1. Merchant processing policy and procedures manuals.

2. Committee minutes for merchant-related activities.

3. Recent reports issued by the bank card associations.

4. Merchant files.

5. Inventory logs for credit card equipment maintained for resale or lease to merchants, including acquisition date, cost, and current value.

6. Agent bank files.

7. All third-party credit files including current financial statements of ISOs/MSPs.

8. All third-party written contracts and agreements, including contracts between ISOs/MSPs and the bank's data processor (if the bank does not have its own in-house operation).

9. All Visa and MasterCard correspondence, including quarterly processing statements, pledge agreements, fraud monitoring reports, and charge-back monitoring reports.

10. Disaster contingency plans for third-party organizations and management's review of the plans.

11. Audit work papers

Appendix C: Profit and Loss Statement
(Sample Only)

Volumes (000s)	**Expenses**
Total sales volume	External data processing
Total transactions	Internal data processing
Average ticket	Research and development
	Terminal expense or depreciation
Income	Personnel
Gross merchant discount	Telephone
Interchange (-)	Occupancy
Assessments (-)	Travel and entertainment
Net merchant discount	Supplies
Interest income	Professional fees
Transaction fees	Fraud and charge-back losses
Terminal fees	Miscellaneous
Miscellaneous fees	
Total income	**Total direct expenses**
Total income per transaction	Total allocated expenses
Return on total income	
Return on total expense	Total expenses
Direct expenses per transaction	Net contribution before tax
Total expenses per transaction (unit cost)	

Appendix D: Merchant File Review Worksheet

Merchant name				
Merchant application				
Signatures				
Business type				
Description of product and services				
Average ticket size				
Volume information				
Social Security/tax ID				
Trade and bank references				
Current processor				
Time in business				
Proper approval				
Site verification				
With photo				
Inspected by				
Credit bureau report				
Evidence of previous merchant activity				
Check MATCH				
Purchase or lease equipment				
Discount Rate				
Swiped transactions (%)				

Appendix E: Merchant Activity and Capital Worksheet

Bank name		**Prior year's data for growth % calculations**
Bank address		
Call report data as of date	**mm/dd/year**	**mm/dd/year**
Tier 1 capital (RC-R)	$	$
Year-to-date (YTD) merchant credit card (cc) sales volume (RC-L)[a]		
Sales for which the reporting bank is the acquiring bank	$	$
Sales for which the reporting bank is the agent bank with risk	$	$
If applicable, aggregate sales of both merchant processing activities	$	$
Acquiring bank		
YTD merchant credit card sales (as acquiring bank) to tier 1 capital	%	
12-month growth rate in merchant credit card sales (as acquiring bank)	%	
Agent bank with risk		
YTD merchant credit card sales (as agent bank with risk) to tier 1 capital	%	
12-month growth rate in merchant credit card sales (as agent bank with risk)	%	
Aggregate (combined merchant processing activity for acquirer and agent bank with risk)		
YTD merchant credit card sales (aggregate) to tier 1 capital	%	
12-month growth rate in merchant credit card sales (aggregate)	%	

[a] The bank may report credit card sales for one of the merchant processing activities or both, depending on the bank's particular merchant processing activities.

Appendix F: Glossary

Acquiring bank (acquirer): A bank that contracts with merchants for the settlement of payment card transactions is an acquiring bank. Acquiring banks contract directly with merchants, or indirectly through agent banks or other third-party organizations, to process card transactions. The acquiring bank generally provides all backroom operations to the agent bank and owns the bank identification number (BIN)/Interbank Card Association (ICA) number through which settlement takes place.

Agent bank: A member of a bank card 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 bank that wants to offer merchant processing as a customer service. Agent banks that participate in an acquiring bank's program only insofar as to refer merchants are known as referral banks. Referral banks typically do not assume liability for merchant losses.

Authorization: An issuing bank's approval of a card transaction in a specific amount. If a merchant complies with bank card association rules in obtaining an authorization, by telephone or electronic terminal, payment to the merchant is guaranteed.

Automated clearing house (ACH): ACH is an electronic network for financial transactions in the United States, which processes large volumes of credit and debit transactions in batches.

Backroom operations: Operational functions performed by the acquirer or issuer to facilitate the day-to-day processing of card transactions (e.g., settlement, fraud, and charge-backs).

Bank card association: A bank card association is an organization, owned by financial institutions, that licenses a bank card program. Visa USA and MasterCard International are bank card associations. Banks must be members of an association to offer the association's card services. Membership rights and obligations are specifically defined by the associations. Both Visa and MasterCard require all members of their organization to be banks.

Bank identification number/Interbank Card Association (BIN/ICA) number: A series of unique numbers used to identify the settling bank for both acquiring and issuing transactions.

Charge-back: Generated when a cardholder disputes a transaction or when the merchant does not follow proper procedures. The issuer and acquirer research the facts to determine which party is responsible for the transaction. Strict card association rules must be followed.

Clearing: Clearing is the process of delivering final transaction data from acquirers to issuers for posting to the cardholder's account. Clearing also includes the calculation of certain fees and charges that apply to the issuer and acquirer involved in the transaction, as well as the conversion of transaction amounts to the appropriate settlement currencies.

Cyber attack: An intentional maneuver to exploit, steal, alter, degrade, destroy, or disrupt computer information systems, networks, software, or infrastructure, or the information that the system processes, stores, or transmits.

Debit card: A card that customers use to pay for a merchant's goods and services. A debit card also enables a user to transact business at an automated teller machine (ATM). In a debit card transaction, the cardholder is accessing funds from a personal checking or savings account.

Discount rate: The fee, as a percent of sales volume, an acquirer charges a merchant for processing sales transactions.

E-commerce: The term used for electronic commerce, which refers to buying and selling products or services using the Internet.

Electronic benefits transfer (EBT): The electronic delivery of government benefits using plastic cards. EBT is an electronic system that allows a recipient to authorize transfer of their government benefits from a federal account to a retailer account to pay for products received. Common benefits provided via EBT in the United States are typically of two general categories, food and cash benefits.

Electronic data capture: Process used when the merchant "swipes" the card through an electronic card reader or terminal. The information on the card's magnetic stripe is entered into the processor's database electronically.

EMV: EMV is a technology that embeds a microprocessor chip on credit cards and debit cards to encrypt transaction data. The technology was jointly developed by Europay, MasterCard, and Visa, and the technology is named for the original developers. EMV technology is widely used in other countries, but not in the United States.

Factoring (credit card factoring): Factoring is used as a method to launder money via credit cards. Factoring, also referred to as credit card factoring, is essentially processing transactions through a merchant account for a business or entity other than the specific business that was screened and set up for the merchant account. Factoring is a form of fraud in which a merchant creates false sales transactions, inflates the sales amount, or alters the sales drafts to receive funds from the issuer. The merchant's intentions could be to obtain additional money to cover charge-backs or cash flow problems, or the merchant may have ceased operations and plans to abscond with the sales proceeds. If the merchant ceases to operate or disappears, the acquirer would be responsible for any remaining charge-backs.

Future or delayed delivery: Sales transactions on products or services that are delivered in the future. Examples of such products or services include airline tickets, concert tickets, and travel/tour packages.

Gift card: A gift card is a card that allows the cardholder to use it for the purchase of goods or services and is used as a nonmonetary gift. Some gift cards can only be used at select retailers, while some can be used anywhere that accepts major credit cards.

High-risk merchant account: A high-risk merchant account poses increased risk to banks through fraud, high charge-back rates, or poor credit history. Examples of merchant account categories that may be deemed high-risk include: businesses where the products incur a high likelihood of consumer fraud; businesses with historically high refund and charge-back rates; businesses that have an elevated risk of bankruptcy; and businesses that sell products or services that are specially regulated by the United States (such as gambling or gaming services or tobacco products).

Holdback: A percentage of the merchant's sales deposits that the acquirer holds back to serve as a reserve against future exposure or to cover existing charge-backs.

Indemnification agreement: An agreement between parties in a contract to protect a party to a contract from liability for wrongdoing or legal issues. Indemnification is common in service contracts and a form of protection from liability for one party in a contract by another party in the contract. Depending on the specific agreement, it may protect from losses, expenses, suits, fines, or judgments.

Independent sales organization (ISO): An organization that provides merchant processing functions on behalf of the acquirer. These functions may include soliciting new merchant accounts, arranging for terminal purchases or leases, and providing backroom services. An ISO and an MSP are functionally similar. The acquirer must register all ISOs/MSPs with the bank card associations. Also, see the definition of MSP.

Interchange: The electronic infrastructure that processes financial and nonfinancial transactions between financial institutions.

Interchange fee: A fee paid by one bank to another to cover handling costs and credit risk in a bank card transaction. The interchange fee, a percentage of the transaction amount, is derived from a formula that takes into account authorization costs, fraud and credit losses, and the average bank cost of funds.

International Standard on Assurance Engagements No. 3402 (ISAE 3402): A global standard for assurance reporting on service organizations.

Laundering: A form of fraud in which a merchant that holds an account with an acquirer submits drafts for a merchant that does not. This is sometimes called draft laundering. The authorized merchant typically receives a percentage of the unauthorized merchant's sales volume. Several states' criminal statutes prohibit laundering.

Member Alert to Control High Risk Merchants (MATCH): Formerly known as the combined terminated merchant file (CTMF), the MATCH file is maintained by the bank card associations based on information reported by acquirers. By checking this file before

approving a merchant, an acquirer determines whether the merchant has a history of poor operating practices.

Member service provider (MSP): A nonmember of MasterCard who markets bank card merchant acceptance on behalf of MasterCard financial institutions. An MSP is functionally similar to an ISO. Also, see the definition of ISO.

Merchant account: A bank account opened by a merchant through a bank or other financial institution that is a member of a major card network.

Merchant bank: For purposes of this booklet, a merchant bank is a bank that provides merchant processing.

Merchant processing: The settlement of credit card or debit card payment transactions by banks for merchants. It is a separate and distinct business line from card issuing. Merchant processing activity, which is off-balance-sheet, involves gathering sales information from the merchant, collecting funds from the issuing bank, and paying the merchant. Various types of third parties may be involved.

Mobile processing (wireless processing): The use of wireless terminals for credit and debit card transactions by merchants.

Monoline Internet merchants: Merchants that provide one single line of business and conduct the business over the Internet, rather than with physical business locations or storefronts for customers to shop and purchase goods and services.

Neural network: In IT, a neural network is a system of programs and data structures that approximates the operation of the human brain. A neural network usually involves a large number of processors operating in parallel, each with its own small sphere of knowledge and access to data in its local memory. Typically, a neural network is initially trained or fed large amounts of data and rules about data relationships. A program can then tell the network how to behave in response to an external stimulus (for example, input from a user who is interacting with the network) or can initiate activity on its own (within the limits of its access to the external world).

Office of Foreign Assets Control (OFAC): The office within the U.S. Department of the Treasury that administers and enforces economic and trade sanctions based on U.S. foreign policy and national security goals against foreign targets, entities, and behavior.

Paper-based transaction: An operation in which the merchant imprints the card and submits paper sales drafts to the acquirer for collection. The paper drafts are sent to the processing center, where they are processed and transferred to magnetic tape for transmission through interchange.

Paydex score: The Paydex is a numerical score granted by Dun and Bradstreet for a business indicating the promptness of their payments to creditors. The Paydex score is calculated

based on a single factor: whether a business makes prompt payments to its suppliers and creditors within agreed-upon terms of payment. The score ranges from zero to 100; a score of 80 or higher is considered healthy. Some banks use this score in their merchant processing activities and it is mentioned in this booklet from that perspective. The OCC does not endorse any specific products.

Payment card: A card that can be used by a cardholder and accepted by a merchant to make a payment for a purchase or in payment of some obligation.

Payment facilitator: Defined by MasterCard, a payment facilitator is a merchant that is registered by an acquirer to facilitate transactions on behalf of sub-merchants. The acquirer is responsible for the actions of the payment facilitator and the sub-merchants. A payment facilitator is operationally similar to a payment service provider.

Payment service provider (PSP): Offered by Visa, the payment service provider is an organization that contracts with an acquirer to provide payment services to sponsored merchants. The acquirer is responsible for the actions of the PSP and the PSP's sponsored merchants. A payment service provider is operationally similar to a payment facilitator.

Prepaid debit card: A type of debit card where the value of the card is preloaded on the card from the funds paid in advance by the consumer. The consumer does not incur debt from the use of the prepaid debit card when the consumer makes a purchase for goods or services.

Referral bank: Agent banks that participate in an acquiring bank's program only by referring merchants are known as referral banks. Referral banks typically do not assume liability for merchant losses.

Rent-a-BIN: An arrangement in which a bank permits an ISO/MSP to use the bank's BIN/ICA number for payment card issuing or merchant processing. In return for allowing the use of the BIN/ICA number by the ISO/MSP, the bank receives a rental fee from the ISO/MSP, hence the term Rent-a-BIN.

Repayable suretyship agreement: In a surety or surety bond, a promise is made by one party to pay a certain amount if the second party fails to meet some obligation, such as fulfilling the terms of a contract. The surety bond protects the obligee against losses resulting from the principal's failure to meet the obligation. A surety is a contract among at least three parties: the obligee (recipient of an obligation), the principal (primary party performing the contractual obligation), and the surety (party that assures the obligee that the principal can perform the task).

Retrieval request: A form used to request a copy of the original sales draft from the merchant. A merchant that fails to send a copy of the sales draft may receive a charge-back. Such charge-backs are not appealable. An issuer may request a copy of the sales draft to verify the signature, to investigate the lack of an imprint, to carry out a cardholder's inquiry, or to look into the possibility of fraud.

Settlement: Settlement is the process of transmitting sales information to the card-issuing bank for collection and reimbursement of funds to the merchant. Settlement also refers to the process of calculating, determining, and reporting the net financial position of issuers and acquirers for all transactions that are cleared. Various third-party organizations may be involved in all aspects of settlement.

Social engineering: The practice of manipulating people into performing actions or divulging confidential information that creates risk exposure for merchant processors and the merchants whose payments they process. Criminals may use social engineering to trick individuals to obtain passwords, bank information, or access to computers and systems and may be a step in a more complex fraud scheme.

Specially Designated Nationals (SDN) List: As part of OFAC's enforcement efforts, the office publishes a list of individuals and companies owned or controlled by, or acting for or on behalf of, targeted countries. The list also includes individuals, groups, and entities designated under programs that are not country-specific. Assets for any individual, company, group, or entity on the OFAC list are blocked, and U.S. persons are generally prohibited from engaging in business with them.

Statement on Standards for Attestation Engagement No. 16, "Reporting on Controls at a Service Organization" (SSAE 16): SSAE 16 is the auditing standard used for service organizations located and operating in the United States.

Termination fees: A merchant account contract written with a bank may require that the term of the contract last a specified length of time. If the contract is terminated by the merchant before the end of the contract with the bank, the bank may charge a termination fee for early cancellation.

Third-party organization: Any outside company with which the acquirer contracts to provide merchant processing services. These services may include network and data transmissions, merchant accounting, backroom operations, sales, or customer service.

References

Laws

12 USC 1464(d)(7), "Regulation and Examination of Savings Association Service Companies, Subsidiaries, and Service Providers" (FSAs)
12 USC 1867(c)(1), "Services Performed by Contract or Otherwise" (national banks and FSAs)

Regulations

12 CFR 3, subpart H, "Establishment of Minimum Capital Ratios for an Individual Bank or Individual Federal Savings Association" (national banks and FSAs)
12 CFR 7.1017, "National Bank as Guarantor or Surety on Indemnity Bond" (national banks)
12 CFR 21.11, "Suspicious Activity Report" (national banks)
12 CFR 160.60, "Suretyship and Guaranty" (FSAs)
12 CFR 163.180, "Suspicious Activity Reports and Other Reports and Statements" (FSAs)
12 CFR 235, "Debit Card Interchange Fees and Routing" (Regulation II) (national banks and FSAs)
12 CFR 1005, "Electronic Funds Transfer" (Regulation E) (national banks and FSAs)
12 CFR 1026, "Truth in Lending" (Regulation Z) (national banks and FSAs)
12 CFR 1005.20, "Requirements for Gift Cards and Gift Certificates" (national banks and FSAs)

Comptroller's Handbook

Examination Process
"Bank Supervision Process"
"Community Bank Supervision"
"Large Bank Supervision"

Consumer Compliance
"Electronic Fund Transfer Act"
"Other Consumer Protection Laws and Regulations"

Safety and Soundness, Other Activities
"Payment Systems and Funds Transfer Activities"

OCC Issuances

Advisory Letter 2002-3, "Guidance on Unfair or Deceptive Acts or Practices" (March 22, 2002) (national banks)
Banking Circular 235, "International Payment Systems Risk" (May 10, 1989) (national banks)

Consumer Advisory 2011-3, "Gift Cards: OCC Provides Tips for Consumers" (October 3, 2011)
OCC Bulletin 1996-48, "Stored Value Card Systems: Information for Bankers and Examiners" (September 3, 1996) (national banks and FSAs)
OCC Bulletin 1998-3, "Technology Risk Management: Guidance for Bankers and Examiners" (February 4, 1998) (national banks and FSAs)
OCC Bulletin 1998-31, "Guidance on Electronic Financial Services and Consumer Compliance: FFIEC Guidance" (July 30, 1998) (national banks and FSAs)
OCC Bulletin 1999-20, "Certification Authority Systems: Guidance for Bankers and Examiners" (May 4, 1999) (national banks)
OCC Bulletin 2002-16, "Bank Use of Foreign-Based Third-Party Service Providers (May 15, 2002) (national banks and FSAs)
OCC Bulletin 2005-35, "Authentication in an Internet Banking Environment: Interagency Guidance" (October 12, 2005) (national banks and FSAs)
OCC Bulletin 2006-34, "Gift Card Disclosures: Guidance on Disclosure and Marketing Issues" (August 14, 2006) (national banks and FSAs)
OCC Bulletin 2006-39, "Automated Clearing House Activities: Risk Management Guidance" (September 1, 2006) (national banks and FSAs)
OCC Bulletin 2008-12, "Payment Processors: Risk Management Guidance" (April 24, 2008) (national banks and FSAs)
OCC Bulletin 2011-12, "Sound Practices for Model Risk Management: Supervisory Guidance on Model Risk Management" (April 4, 2011) (national banks and FSAs)
OCC Bulletin 2011-26, "Authentication in an Internet Banking Environment: Supplement" (June 28, 2011) (national banks and FSAs)
OCC Bulletin 2011-27, "Prepaid Access Programs: Risk Management Guidance and Sound Practices" (June 28, 2011) (national banks and FSAs)
OCC Bulletin 2012-16, "Capital Planning: Guidance for Evaluating Capital Planning and Adequacy" (June 7, 2012) (national banks and FSAs)
OCC Bulletin 2012-34, "Supervision of Technology Service Providers: FFIEC IT Examination Handbook Booklet Revision and Administrative Guidelines for Interagency Supervisory Programs" (October 31, 2012) (national banks and FSAs)
OCC Bulletin 2013-29, "Third-Party Relationships: Risk Management Guidance" (October 30, 2013) (national banks and FSAs)

Other

FFIEC Bank Secrecy Act/Anti-Money Laundering Examination Manual

FFIEC Information Technology (IT) Examination Handbook
"Outsourcing Technology Services"
"Information Security"
"Business Continuity Planning"
"Retail Payment Systems"
"Supervision of Technology Service Providers"

National Automated Clearing House Association (NACHA)
"NACHA Operating Rules & Guidelines"

American Institute of Certified Public Accountants, Accounting Standards Board
Statement on Standards for Attestation Engagement No. 16, "Reporting on Controls at a Service Organization" (SSAE 16)

International Auditing and Assurance Standards Board
International Standard on Assurance Engagements (ISAE 3402)