Comptroller's Handbook for National Bank Examiners
April 1992 - Temporary Insert

Merchant Processing
Introduction
Section 212A.1

Merchant processing is the settlement of credit card sales transactions for merchants. It is a separate and distinct business line from credit card issuing. Banks offering merchant processing are called "acquiring" banks. A credit card issuing bank issues the credit card and carries the credit card loan. An acquiring bank settles with the merchant for credit card transactions. Most merchant processing activity is off-balance sheet.

Acquiring banks contract directly (or indirectly through agent banks or other third parties) with merchants to process their credit card transactions. The acquiring bank collects the funds from the card issuing bank and credits the merchant's account. The acquiring bank charges the merchant a discount fee, usually based on the amount and number of sales transactions. Merchants clear their sales transactions by submitting the paper sales drafts physically or transmitting the sales information electronically by a dial terminal. To hasten the collection of funds, most merchants now submit their sales transactions electronically. In a typical electronic sales transaction, the salesperson "swipes" the credit card through an electronic card reader. The information on the card's magnetic stripe is entered into the processors' data base. It is then transmitted to the issuing bank for authorization.

Merchants obtain approval for credit card transactions from an issuing bank or another third party approved by the card issuer. This process is called authorization, and acquiring banks provide this service to their merchants. Authorizations prevent transactions over a cardholder's credit limit (or the use of identified, stolen or fraudulent cards). Acquiring banks assign merchants an authorization limit, over which individual sales transactions must be approved. The merchant can obtain authorizations by phone or electronically by a dial terminal.
After the transaction is authorized, the sales person enters the sales information through a terminal, often an electronic cash register. At the end of the day, the merchant batches (or totals) all credit card sales and transmits the data to the acquiring bank or third party processor. The acquiring bank transmits the information to the issuing bank, obtains the funds, and credits the acquiring bank's clearing account. In an electronic transaction, the acquiring bank may settle with the issuing bank by the day following the merchant's submission. Paper transactions lengthen the settlement process by several days.

Electronic technology has generated a change in the makeup of banks' merchant bases by allowing them to deal with merchants thousands of miles away. Although this increases the profit potential of merchant departments, it also increases the risk. Banks no longer have the benefit of proximity to monitor a merchant's business activities. This is true even for community banks. Previously a paper-based industry, merchant processing departments required large staffs and expensive equipment; hence, regional and multinational banks dominated the industry. Technology has revolutionized the industry by reducing the costs and labor needed to process merchant transactions. As a result, community banks are now active players in the market.

The volume of business handled through electronic systems has grown rapidly and most credit card sales are now cleared electronically. Electronic transmission increases risk over the paper-based system because of the volume and speed of transactions. If not properly monitored, millions of dollars of fraudulent transactions can be entered into the credit card system quickly. Most merchant processing activity is off-balance sheet. In banks with nation-wide merchant portfolios, the merchants' funds are wired each day to their local deposit account. Banks can process millions of dollars a month with little change apparent in their balance sheets. There are no specific risk- based capital allocations for this activity. However, banks that engage in merchant processing must maintain capital bases consistent with the risk in this activity. The examiner should encourage bank management to set limits on the amount of sales volume they will process. This amount should correlate with the capital structure of the bank, expertise of management, and risk profiles of the merchant portfolio.

Merchant processing can be a profitable business for the bank. However, the business poses significant risk if not properly controlled. Merchant processing is characterized by thin profit margins and high transactional and sales volumes. Acquiring banks can incur losses through merchant fraud, merchant bankruptcy, or poor product pricing. Banks also have incurred losses through their failure to monitor the activities of Independent Service Organizations (see below).

Policies and Procedures

Any bank participating in merchant processing must be fully aware of the risks involved. The board must provide sound policies, establish proper procedures, develop good internal controls and audit procedures, and maintain adequate blanket bond coverage. To monitor the condition of the department, the policy should require adequate reporting systems to management and the board.

Merchant Risk

The primary risk in dealing with merchants comes from customer chargebacks. Chargebacks are generated when a customer is unhappy with the merchandise, never received the merchandise, or never authorized the charge and is unable to resolve the problem with the merchant. In these instances, the customer may request a chargeback to his or her account. The acquiring bank must research the dispute. If the dispute is legitimate, the purchase is credited back to the customer's credit card account and charged back to the merchant. Generally, the customer has four months after a credit card purchase to dispute the purchase. After the customer dispute is made, the resolution process can take up to another six months. Therefore, when a bank processes sales transactions for a merchant, the contingent liability of chargebacks can span sales for the prior 10-month period or sometimes longer.

Chargebacks may result from deliberate merchant fraud. For instance, the merchant may sell deceptive or misleading merchandise or never deliver the merchandise to the customer. This activity often results in a large volume of chargebacks from the consumers. If the merchant is unable to honor the chargebacks, the acquiring bank must absorb the losses. In other cases, the merchant may launder drafts for another merchant who cannot submit them directly because of his past record (this practice is also known as factoring). These drafts are generally high risk and result in a large volume of chargebacks.

The financial condition of the merchant could have a significant impact on the chargeback exposure to the bank. If the merchant sells a future service product, declares bankruptcy, and never fills customers' orders, the bank could have significant chargeback exposure. In these cases, the bank would probably be treated as an unsecured creditor. Financially strapped merchants are also more vulnerable to factoring schemes or other fraudulent activity.
To control merchant risk, the bank must implement a merchant underwriting policy. The policy should require an initial background check of the merchant, to support the validity of the business, creditworthiness of the merchant and previous sales activity. The bank's underwriting standards for merchants should require at a minimum:

- A credit bureau report on the principal of the business.
- A financial statement or tax return on the business if the volume of activity is significant.
- Evidence of previous merchant activity, such as recent monthly statements from the previous processor.
- An onsite inspection report, including a photograph of the business.
- A signed merchant application listing type of business, location, principal, etc.
- A signed merchant processing agreement.
- An estimate of merchant's projected sales activity (e.g., average ticket size, daily/monthly sales volume).
- A copy of the corporate or partnership resolution, if applicable.

When evaluating the credit quality of a merchant, a bank must also consider the line of business. A merchant offering low quality products or services may incur a higher incidence of chargebacks. Some types of businesses are inherently more risky. For example, although there are many reputable mail order and telemarketing merchants, these areas have, in the aggregate, displayed a much higher incidence of chargebacks. Also the risk of chargeback is greater if the merchant sells goods or services for future delivery, such as airline tickets, health club memberships, or travel clubs. This is because timeframes for many of the remedies available to a customer begin to run from the date of delivery of goods and services. Holdback or reserve accounts may be necessary to protect the bank in those cases.

The financial condition of high volume merchants should be monitored on an ongoing basis. Because the financial statements of these merchants are more complicated, they should be reviewed by persons with commercial credit experience. If credit information shows deterioration in the merchant's financial condition, the bank should reduce its risk exposure. For instance, when dealing with a financially unstable merchant, the bank may require a holdback or security deposit.

In addition to monitoring the financial condition of each merchant, a bank should also have a system to monitor daily merchant activity. A bank's ability to detect fraudulent merchant activity quickly is important in controlling losses. A bank should not rely on excessive chargeback activity to identify fraud. Often, the fraud is already well established. Available monitoring systems can detect fraud almost instantaneously and prevent release of funds to the merchant.

The primary tool of a bank's fraud detection system is the exception report. It is generated from parameters based on expected merchant activity. Any activity outside these parameters is investigated by the bank to determine if fraud is involved. For example, a dramatic increase in daily sales volume may indicate laundering. To be most effective, exception parameters should be tailored to each merchant's expected sales activities. Examples of common exception parameters include average ticket size, daily volume, multiple tickets of same dollar amount, multiple use of same cardholder number, and keyed versus swiped transactions.

Settlement Risk

Settlement is the process of transmitting sales information to the card issuing bank for collection and reimbursement to the merchant. In a typical transaction, the merchant submits sales information to the acquiring bank or third party processor. The sales information is then transmitted through interchange to the issuing bank. Interchange is the system controlling exchange of data between acquiring banks and issuing banks. In "on-us" transactions, the acquiring and issuing bank are the same and the transaction does not flow through interchange. Although failure to settle rarely occurs, it can result in significant financial risk to the bank. Failure to settle can occur anywhere in the funds transfer function. For example, an issuing bank could fail and not fund merchant charges. Or, a processing center could fail and not transmit sales information to the issuing bank for collection. To control settlement risk, the bank should ensure that written agreements are in place with all parties involved in the settlement process. The agreements should detail specific responsibilities and payment arrangements. When using the services of third party processors, the bank should obtain copies of the processor's disaster contingency plans. The bank should also ensure that the processor receives regular external audits that check for adequate internal controls.

Independent Service Organizations

Independent service organizations (ISOs) have assumed a significant role in the merchant processing industry. An ISO may also be called a member service provider or third party marketer. ISOs can perform a variety of functions for a bank, including soliciting merchants, providing customer and accounting services, and selling and servicing electronic terminals. ISOs must deal either directly with a bank or indirectly with a bank through another ISO.
Because these organizations represent the bank, bank management must be thoroughly familiar with the reputation, experience, and financial capacity of each ISO and its principals. Background checks should be conducted on the principals of each ISO to determine their good standing. The financial capacity of the ISO and its principals should also be analyzed to support the organization's continued viability and capacity to absorb losses. Because most ISOs rely heavily on sales commissions, they may sometimes overlook merchant quality. As a result, some banks require specific reserves from ISOs to absorb losses due to merchant fraud or chargebacks. Separate files should be maintained for each ISO. At a minimum, these files should include:

- A current financial statement on the principal and the ISO. The type and detail of the financial statement should relate to the size of the company.
- A detailed onsite inspection of the ISO performed by a bank employee.

- Evidence of a check of bank and trade references.
- A credit report on the principal of the ISO.
- A background investigation (including a check for prior criminal convictions) on the principal of the ISO.

In several cases, banks have incurred significant losses from their failure to control the activities of ISOs. Although banks can delegate a substantial amount of the day-to-day operational activities to an ISO, they retain full liability for the ISO's actions. Therefore, a bank must have adequate systems in place to monitor the activities of ISOs to ensure they are operating within the guidelines established by the bank.

In the past, ISOs were sometimes involved in the settlement process. Cases of ISOs failing to settle with merchants caused VISA and MasterCard to issue regulations preventing ISOs from being involved in the funds transfer process.

Written contracts with ISOs should specifically explain their responsibilities, compensation arrangements, and allowable uses of the bank's name. All legal contracts should be reviewed by the bank's counsel. Because merchant processing is a specialized industry, the bank should use counsel that is familiar with this type of activity.

Agent Banks

Acquiring banks often process credit card transactions for other banks, known as agent banks. Typically, agent banks are liable for any losses incurred on their merchant accounts. Acquiring banks should ensure that agent banks are fully aware of their financial liability for merchant account losses. Usually, acquiring banks apply their own merchant underwriting standards to agent bank merchant applications. On occasion, acquiring banks will accept an agent bank merchant that does not meet their underwriting standards. In these cases, the acquirer should ensure that the agent bank is aware of the risks involved in the merchant relationship. The risk may be conveyed through a separate indemnification agreement signed by a senior officer in the agent bank.

Acquiring banks should review periodically the financial condition of agent banks. The financial condition of the agent bank should be consistent with the risk profile of its merchant portfolio and volume of merchant activity.

Data Processing Vendors

Banks often find it cost effective to use the services of third party data processors for merchant processing services. The processors primarily provide accounting and authorization services. Generally, these processors assume no liability for merchant losses. Banks should have written contracts in place with these processors that specifically explain the responsibilities and payment arrangements. See the Federal Financial Institutions Examination Council EDP Handbook under the "EDP User and Servicer" section for more information on data processing vendors.

Pricing/Profitability

Banks must have adequate systems in place to measure the profitability of the merchant processing department. Competition for merchant business has eroded discount fees. Profit margins are extremely thin. As a result, only efficiently run, high volume departments can operate profitably. Systems should be available to measure overall profitability of the department including all direct and indirect costs. Also, the bank should generate reports on individual merchant profitiability.

Banks should adopt pricing policies to set minimum discount rates for merchants based on their volume of sales activity, inherent risk in operations, and overall financial condition. Often banks give merchants a favorable discount rate because of existing commercial loan or deposit relationships. Although this is an acceptable practice, a bank should be able to measure the overall profitability of the merchant's account. This will ensure that the merchant's other bank relationships offset the favorable discount rate.

When the bank is contracting with an ISO, the ISO often determines the discount rate charged to the merchant. The bank receives an agreed upon percentage of each sales transaction. To acquire new merchants, the ISO may use lower rates. If the discount rates do not cover the costs of the ISO's overhead expenses, it could jeopardize their financial condition. Banks should review periodically the discount rates set by their ISO to ensure that they adequately cover the ISO's operating costs.

Banks should not offer favorable discount rates to insiders or their related interests. The examiner should review discount rates for these individuals to ensure they are the same rates and terms offered to other bank customers.

Merchant Processing
Examination Objectives
Section 212A.2

1. To determine if policies, practices, procedures and internal controls regarding merchant processing are adequate.

2. To determine if bank officers and employees are operating in conformance with established guidelines.

3. To evaluate the portfolio for collectibility and profitability.

4. To determine the scope and adequacy of the audit function.

5. To determine compliance with applicable laws, rulings, and regulations.

6. To initiate corrective action when policies, practices, procedures or internal controls are deficient or when violations of laws, rulings, or regulations are noted.

Merchant Processing
Examination Procedures
Section 212A.3

1. Complete or update the Merchant Processing section of the Internal Control Questionnaire.

2. Based on the evaluation of internal controls and work performed by the internal/external auditors, determine the scope of the examination. Select from among the following examination procedures those steps that are necessary to evaluate the merchant processing department of the bank.

3. Test for compliance with policies, practices, procedures, and internal controls in conjunction with performing the selected examination procedures. Obtain a listing of any deficiencies noted in the latest review done by internal/external auditors. Determine if management has taken corrective action.

4. Perform appropriate verification procedures (See Credit Card Plans-Verification Procedures).

5. Request the bank to supply copies of the:

    a. Organizational chart for the department.

    b. Resumes of all principals in the department.

    c. Job descriptions of all principal positions.

    d. Strategic plans and budgets for the department.

    e. Merchant processing policy and procedures manual.

    f. Flow chart of the settlement process.

    g. Name, address, and current financial statements of ISO(s) used by the bank.

    h. Profitability report for the department for the previous year and year-to-date.

    i. Most recent internal/external audit report and management's response.

    j. Agent bank agreement.

    k. Merchant agreement and application.

    l. Name and account numbers of general ledger accounts relating to merchant processing.

m. Name and location of data processing vendor, if applicable.

6. Request that the bank have the following information available for the examiner's review:

   a. Reports routinely reviewed by department management and the board of directors.

   b. Reports detailing total number of merchants, daily/monthly/annual volume of sales by

   c. volume, and number of transactions.

   d. All contracts between ISOs and the bank, including contracts between the data processor, if the bank does not have its own in-house operation.

   e. Merchant, ISO, and agent bank files.

   f. If the ISO(s) has access to the bank's data processing system, a list of access codes assigned to ISO personnel.

   g. Account profitability statements on a representative sample of individual merchants. The examiner may want to request this for the bank's larger merchants (e.g., top 50 merchants). Examiners should also review any insider related merchant businesses for instances of preferential pricing.

   h. Copy of the bank's daily fraud monitoring reports.

   i. Copy of the bank's daily exception reports.

   j. Inventory logs for credit card equipment inventory the bank keeps for resale or lease to merchants.

   k. Status report on the aging of chargebacks and an aging trend report on chargebacks.

   l. Name and address of agent banks.

   m. Trial balance of all merchants serviced by the bank along with daily sales volume.

   n. Disaster contingency plans for third party vendors.

Management

1. Review the resumes of the principals in the merchant processing department to:

   a. Determine if the staff has adequate experience in merchant discount processing.

   b. Determine if merchant approval personnel have credit experience.

2. Compare staffing levels with the volume of business in the department, number of merchant applications reviewed daily, etc. Determine if current staffing levels are appropriate in consideration of present and future plans.

3. Review staff turnover and determine if turnover appears excessive.

4. Review the bank's strategic plan and determine if management's plans for the department are clear and represent the current direction of the department.

5. Review internal MIS reports and determine if they adequately inform management of the condition of the department.

Merchant Underwriting Standards

1. Select a representative sample of recently approved merchant files (for example, within last 90 days). The sample should include merchants obtained directly by the bank, through ISOs, and through agent banks. Review the sample of merchant files for compliance with the policy. At a minimum, the files should contain:

   a. A credit bureau report on the principal of the business.

   b. A financial statement or tax return on the business, if merchant volume is significant.

   c. Sales tax number for the business.

   d. Evidence of previous merchant activity.

   e. Onsite inspection report, including a photograph of the business.

   f. Signed merchant agreement between the bank and the merchant.

   g. Estimate of the merchant's projected sales activity (i.e. average ticket size, daily sales volume).

   h. Merchant application listing type of business, location, principal, etc.

   i. Corporate resolution, if applicable.

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

3. Select several merchant reserve accounts and review for compliance with the merchant contract.

4. Determine how the bank documents exceptions to the merchant approval policy.

Settlement Process

1. From the review of the settlement flow chart, determine the flow of funds and all parties involved in the settlement process.

2. Review contracts of all vendors involved in the settlement process and determine financial liability of all parties.

3. Determine the percentage of merchant sales transmitted electronically vs. paper.

4. Review reasonableness of contingency plans for all parties involved in the settlement process.

5. If ISOs perform merchant servicing tasks, review the reasonableness of their contingency plans.

Chargeback Processing

1. Evaluate the adequacy of the chargeback system to determine if the system:

    a. Is automated or manual.

    b. Can quantify outstanding chargebacks and their age.

    c. Can prioritize the chargeback research process.

    d. Can measure the efficiency of the chargeback process.

2. Review the trend in the volume and aging of chargebacks. Investigate significant trends in both the volume and age of chargebacks and:

    a. Discuss with management any merchants that are generating significant chargebacks.

    b. Instruct the bank to charge off any chargebacks aged over 90 days.

3. Determine if the bank has suffered any significant losses from merchant chargebacks over the past several years.

4. Determine how the bank reports merchant chargeback losses on the general ledger.

5. Determine if the bank has a policy for charging off stale chargebacks.

6. Determine how the bank evaluates the adequacy of its chargeback systems. Inquire how the bank plans for contingencies, such as large merchant bankruptcies which generated a large volume of chargebacks.

Independent Service Organizations

1. Review a sample of ISO contracts and check for compliance with the policy. The contracts should:

    a. Detail the financial compensation and payment arrangements.

    b. Tie fees to performance (e.g., number of merchants, volume of sales transactions, chargeback activity).

    c. Require security deposits by the ISO to offset potential merchant losses. These deposits should bear a reasonable correlation to the level of sales volume generated by the ISO.

    d. Include remedies to protect the bank if the ISO fails to perform (include indemnity and early termination rights).

    e. Require all monetary transactions to be handled directly between the bank and the merchant.

    f. Prohibit the ISO from assigning the agreement or delegating responsibilities to any other party.

    g. Provide for criteria of acceptability of merchants.

    h. Specify who owns merchant relationships.

    i. Control the future use and solicitation of merchants.

    j. Define the allowable use of the name, trade name, and logo of both the bank and the ISO(s).

    k. Cover the frequency and means of communication and monitoring of each party.

    l. Describe the recordkeeping each party must maintain and allow the other party access to the records.

    m. Specify the frequency and type of financial statements to be required of the ISO.

    n. Warranty that all federal consumer laws are followed.

    o. Address handling and responsibility for merchant chargebacks.

    p. Provide for onsite inspections by bank employees.

2. Review a representative sample of ISO credit files and check for compliance with policy. At a minimum, the files should contain:

    a. A current financial statement on the principal(s) and the ISO. The type of financial statement should correlate to the size of the company.

    b. A detailed onsite inspection of the ISO performed by a bank employee.

    c. Evidence of a check of bank and trade references.

    d. A credit report on the principal(s) of the ISO.

    e. A criminal check on the principal(s) of the ISO.

3. Analyze the financial stability of the ISO(s). Determine if ISO reserve accounts are consistent with the condition of the company and the volume of business they generate.

4. Review the bank's procedure for monitoring the activities of ISO(s).

5. Review system access codes assigned to ISO personnel. Determine if access capabilities are reasonable depending upon the persons' responsibilities.

Fraud Detection

1. Review the bank's fraud detection system. Determine which persons perform fraud detection and the type of training they have received.

2. Determine if the scope and frequency of the fraud review is adequate.

3. Determine how the bank derives parameters for fraud reports.

4. Determine the bank's course of action if it detects suspicious merchant activity.

Audit

1. Review the internal/external audit report. Determine if management has addressed audit findings.

2. Review the scope of the internal audit to determine that it addresses all operational areas (see ICQ).

3. Determine the internal/external auditor's knowledge of the merchant processing area.

Credit Card Equipment

1. Review the security over inventory kept for merchants. Review inventory logs for timeliness and completeness.

Agent Banks

1. Determine if the bank has an agent bank policy. Does the policy address:

    a. Agent bank acceptance.

    b. Agent bank merchant underwriting.

    c. Policy exceptions.

    d. Agent bank liability.

2. Obtain a report which shows agent bank merchant volume by agent bank. Review agent banks that appear to have significant merchant volume in comparison to the size of each of their banks.

3. Review a sample of agent bank files. Evaluate the adequacy of information and check for compliance with policy.

4. Determine if the bank periodically reviews the financial condition of agent banks.

Pricing/Profitability

1. Review the department's profitability statements. Compare to the budget and investigate significant variances.

2. Determine the bank's pricing policy.

3. Review a sample of merchant profitability statements. Investigate reasons for low profitability or actual losses.

4. Review a sample of merchant profitability accounts and compare actual pricing against the pricing policy.

Comptroller's Handbook for National Bank Examiners
April 1992 - Temporary Insert

Merchant Processing
Internal Control Questionnaire
Section 212A.4

Policies and Procedures

1. Has the board of directors, consistent with its duties and responsibilities, adopted written merchant processing policies that:

   a. Establish clear lines of authority and responsibility?

   b. Identify the risks and limit the amount of risk the bank is willing to accept?

   c. Place limits on the individual and aggregate volume of the bank's merchant activity?

   d. Assume that adequate and knowledgable staff is provided?

   e. Require written contracts between all third parties?

   f. Establish criteria for the acceptance of merchants?

   g. Require the development of procedures to monitor the activity of each merchant?

   h. Address cases when merchant reserve (holdback) accounts are appropriate?

   i. Establish guidelines for the periodic review of merchant creditworthiness?

   j. Develop criteria for contracting with any ISO to act as agent for the bank?

   k. Require the development of adequate MIS systems to keep management and the board informed of the condition of the program?

   l. Require that a comprehensive procedures manual be developed to guide officers and employees in administering the program?

   m. Establish guidelines for handling exceptions to policy?

   n. Establish guidelines for the acceptance of agent banks?

   o. Require review of all contracts and applications by legal counsel familiar with merchant discount 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:

   a. Establishing new business?

   b. Monitoring existing business?

   c. Dealing with ISOs?

   d. Handling complaints from merchants?

   e. Conducting settlement procedures and wire transfers?

   f. Processing merchant chargebacks?

   g. Training new personnel?

Management

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

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

3. Are separate, pro-forma budgets prepared for the department?

4. Has the board reviewed the bonding needs of the department?

Merchants

1. Does the merchant approval policy provide for clear and measurable underwriting standards for merchants?

2. Does the bank require written merchant applications?

3. Does the bank perform onsite inspections on all merchants?

4. Are inspections written and do they include a photograph of the merchant's business?

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

6. Does the merchant approval policy address:

   a. Desirable vs. undesirable merchants?

b. Merchant file documentation requirements?

c. Officer merchant approval authorities?

d. Merchant underwriting guidelines?

e. Merchant termination procedures?

f. Handling exceptions to the merchant approval policy?

g. 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 on all large merchants reviewed at least annually?

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

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

Settlement Process

1. Does the bank settle directly with the merchant?

2. Can the bank hold merchant funds pending the resolution of suspected fraudulent activity?

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

4. Are payments to merchants made only against collected funds?

5. Is access to merchant and ISO reserve accounts restricted to bank personnel?

6. Are merchant and ISO accounts reviewed periodically for suspicious activity?

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

8. If ISOs perform accounting and servicing functions, have contingency plans been developed to cover their services?

Chargeback Processing

1. Are policies and procedures in place for chargeback processing?

2. Can the bank generate reports on:

   a. Daily chargeback activity?

   b. Status and aging of chargebacks?

   c. Exception reports on merchants experiencing unusual chargeback activity?

3. Are losses from merchant chargebacks clearly identified on the general ledger?

Independent Service Organizations

1. Does the ISO underwriting policy address minimum standards for:

   a. The financial condition of the ISO?

   b. The type and timing of financial information to be provided by the ISO?

   c. Periodic bank review of ISO financial information?

   d. ISO management depth and experience?

2. Does the policy require background checks, including criminal records of all ISOs and their principals?

3. Does the bank require bank and trade references on all ISOs and their principals?

4. Does the bank require specific reserve accounts from ISOs to absorb losses from merchant chargebacks or other damages?

5. Has the bank registered all ISOs with VISA/MasterCard?

6. Does the bank review all promotional material used by ISOs?

7. Does the bank attend sales training sessions for ISO salespersons?

8. Does the bank call back merchants periodically to discuss ISO sales methods, customer service, etc.?

9. For subcontracted ISOs, does the bank require written contracts between the bank and the subcontracted ISO?

10. Has the bank performed onsite inspections of all bank ISOs, including subcontracted ISOs?

11. Does the bank regularly review the propriety of system access codes for those ISOs with access to the bank's data processing system?

12. Are all system change requests required to have prior approval of a bank employee?

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 variances of:

    a. Average ticket size?

    b. Daily volume?

    c. Multiple same dollar amount of tickets?

    d. Keyed vs. swiped transactions?

    e. Multiple use of same cardholder number?

Audit

1. Does the department receive audit coverage?

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

3. Does the scope of the audit address:

    a. All operational areas?

    b. Compliance with policy?

    c. Compliance with VISA/MasterCard regulations?

    d. Compliance with written contracts?

    e. Overall risk in the area?

4. Does the bank require that all ISOs have operational audits?

5. For ISOs performing servicing tasks, does the bank require an EDP audit of the ISOs' systems?

Credit 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?

Agent Banks

1. Are agent bank agreements in writing?

2. Are agent banks informed of their financial liability for merchant fraud?

3. Are merchants obtained through agent banks subject to the same underwriting standards as direct or ISO 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 agent bank acceptance policy address:

   a. Financial condition of the bank?

   b. Early termination of the agent bank relationship if the bank suspects unsafe and unsound activities?

Pricing/Profitability

1. Does the bank's pricing system address:

   a. Employee costs, including educational or training costs, to ensure staff competency?

   b. Cost of computer hardware, software, and dedicated phone lines if the bank provides its own back room operations?

   c. Cost of funds to provide float to the clearing process?

   d. Insurance and bonding needs?

   e. Loss history and the risk of future loss?

   f. Annual budget and strategic plans?

2. Do department profitability reports include both direct and indirect costs?