

CREDIT CARD RELATED MERCHANT ACTIVITIES

Core Analysis Decision Factors

Examiners should evaluate Core Analysis factors to determine whether Expanded Analysis is necessary. Click on the hyperlinks found within each of the Core Analysis Decision Factors to reference the applicable Core Analysis Procedures.

Do Core Analysis and Decision Factors indicate that risks are appropriately identified, measured, monitored, and controlled?

C.1. Are policies, procedures, and risk limits adequate? Refer to Core Analysis [Procedures #2-3](#).

C.2. Are internal controls adequate? Refer to Core Analysis [Procedures #4-7](#).

C.3. Are the audit or independent review functions adequate? Refer to Core Analysis [Procedures #8-10](#).

C.4. Are controls over merchants, agent banks, and Independent Sales Organizations (ISOs) adequate? Refer to Core Analysis [Procedures #11-47](#).

C.5. Does management properly monitor and control chargebacks? Refer to Core Analysis [Procedures #29-32](#).

C.6. Are reserves for chargebacks adequate? Refer to Core Analysis [Procedure #31](#).

C.7. Are information and communication systems adequate and accurate? Refer to Core Analysis [Procedures #48-50](#).

C.8. Do the board and management effectively supervise this area? Refer to Core Analysis [Procedures #51-54](#).

CREDIT CARD RELATED MERCHANT ACTIVITIES

Core Analysis Procedures

Examiners are to consider the following procedures but are not expected to perform every procedure at every bank. Examiners should complete only the procedures relevant for the bank's activities, business model, risk profile, and complexity. If needed, based on other identified risks, examiners can complete additional procedures. References to laws, regulations, supervisory guidance, and other resources are not all-inclusive.

Preliminary Review

1. Consider the following factors when determining the scope of the review of Credit Card Related Merchant Activities:

- **The significance that merchant activities play in an institution's overall strategic plans and budgeting process;**
- **The total-dollar sales volume of credit card related merchant activities processed and the number of merchants;**
- **Whether merchants are concentrated in one industry or geographic area that may pose increased risk to the financial institution;**
- **The bank's capital structure;**
- **Whether activities are conducted primarily to accommodate existing customers or if they represent a significant activity for the bank;**
- **Management expertise as reflected in previous examination reports, audit reports, and other correspondence; and, any remedial action taken by management to correct any deficiencies noted;**
- **Use of third party service providers that provide merchant processing activities; and, the adequacy of management's oversight of third parties (as reflected in prior audits and examinations);**
- **Use of Independent Sales Organizations (ISOs);**
- **Risk profiles of the merchants (examples of higher risk profiles include mail order businesses, telemarketing, retailers selling goods or services for future delivery, and merchants selling low-quality products or services);**
- **Prior losses from, and trends in the volume of, merchant chargebacks and unreconciled items in the settlement account; and**
- **Any contingent liabilities arising from the bank's processing activities.**

Policies, Procedures, and Risk Limits

2. Determine whether merchant processing policies adequately establish:

- **Lines of authority and responsibility;**
- **Risk-assessment and fraud-detection procedures;**
- **Cardholder information security standards;**
- **Risk identification practices and limits on the amount of risk the bank is willing to accept;**
- **Limits on individual and aggregate volumes and/or concentrations of merchant activity (management should set limits on the amount of sales volume processed that correlates with merchants' risk profiles and the bank's management expertise and capital structure);**
- **Requirements for written contracts between all third parties;**

- **Due-diligence criteria for initially accepting merchants and periodically reviewing merchants' creditworthiness;**
- **Due-diligence criteria for initially ensuring, and periodically reviewing, third party compliance with Association (Visa and MasterCard) requirements regarding issues such as registration, contract provisions, audit accessibility, etc.;**
- **Guidelines for monitoring merchant activities and assessing their information-security practices;**
- **Criteria for determining the appropriateness of merchant reserve accounts;**
- **Criteria for contracting with any ISO to act as agent for the bank;**
- **Guidelines for acquiring or issuing rent-a-bins (see [Procedure 34.](#));**
- **Guidelines for handling policy exceptions;**
- **Guidelines for accepting agent banks;**
- **Pricing policies; and**
- **Requirements for legal reviews of all contracts and applications (by legal counsel familiar with merchant processing).**

Note: Formal policies may not be necessary for banks with minimal merchant activity. Institutions are expected to assess the risks posed by individual merchants on a case-by-case basis and to implement controls to manage relationships commensurate with identified risks.

3. Determine whether the merchant-processing procedures manual appropriately provides for:

- **Establishing new business relationships;**
- **Monitoring existing relationships for credit and financial exposures;**
- **Monitoring potential or existing concentrations (for example, by merchant type/industry, geographic location, or processing volumes by one merchant);**
- **Dealing with ISOs;**
- **Handling complaints from merchants;**
- **Performing settlement procedures that include clearing items in a timely fashion;**
- **Processing merchant charge-backs; and**
- **Training new and existing personnel.**

Note: Banks with minimal activity may not need a formal procedures manual.

Internal Controls

4. Review recent risk assessments relating to merchant activities and determine whether internal and external threats are identified and appropriate controls are in place. Consider whether the bank uses:

- **Appropriate risk rating processes (using internal metrics or industry codes); and**
- **Reports that clearly display the types of merchants they serve and the risks involved, (including information on whether the merchants are generally swipe, keyed, or chip merchants).**

5. Determine whether the board and senior management regularly review pertinent merchant activity (using reports, dashboards, or other mechanisms that provide information commensurate with the

level of merchant risks).
6. Determine whether adequate separation of duties (or compensating controls) exists in sensitive areas such as: <ul style="list-style-type: none"> • Preparation of input and reconciliation of output, and • Merchant acquisitions/approvals.
7. Determine whether appropriate procedures are in place to prevent, detect, and respond to policy and procedural exceptions.
Audit or Independent Review
8. Review internal and external audit reports to identify any concerns relating to merchant processing.
9. Determine whether the board and management regularly review audit reports and Association correspondence and appropriately respond to audit findings and Association concerns.
10. Review the scope, frequency, and adequacy of the audit function and determine whether all merchant processing areas are addressed. <i>Note: Effective audit programs will identify contraventions of internal policy, Association regulations, and written contracts; and ensure timely settlement balancing.</i>
Merchant Underwriting Standards and Monitoring Procedures
11. Evaluate practices designed to ensure compliance with the merchant-approval policy. <ul style="list-style-type: none"> • To assess compliance with policy guidelines, review a sample of files for recently approved merchants. The sample should include, when applicable, merchants solicited directly by the bank, through ISOs, and through agent banks. The merchant-approval policy should provide clear and measurable underwriting standards for merchants. Verify that standards are maintained and files contain, at a minimum, the following items: <ul style="list-style-type: none"> ○ Merchant applications listing the type of business, location, principal(s), and other relevant structure information; ○ Merchant processing agreements that detail all pertinent activities; ○ Corporate resolutions, if applicable;

<ul style="list-style-type: none">○ Onsite inspection reports;○ A credit bureau report on the principal(s) of the business;○ Documentation of the bank checking prospective merchants against the Member Alert to Control High Risk Merchants (MATCH) system;○ Financial information on the business (typically received annually);○ Sales tax number for the business (tax ID number);○ Evidence of review of previous merchant activity (recent monthly statements from the previous processor); and○ Estimate of the merchant's projected sales activity. <ul style="list-style-type: none">● Verify that management determines why a merchant has or is switching banks (could indicate excessive charge-backs with previous processor).
12. Select a sample of merchant reserve accounts and review for compliance with merchant contracts and Association requirements.
13. Determine whether exceptions to merchant approval policies are approved, reasonable, and documented.
14. Determine whether merchant applications are reviewed by a person who has adequate credit experience.
15. Determine whether the acquiring bank maintains a list of restricted merchants. Characteristics that banks consider when determining restrictions may include: <ul style="list-style-type: none">● Business plans, types of merchandise or services offered, and marketing practices; and● Order, shipping, and return policies.
16. Determine whether underwriting activities, monitoring procedures, and management information systems (MIS) adequately consider or include: <ul style="list-style-type: none">● Sale volumes and product delivery periods;● Projected and actual ticket sizes;● Card-not-present transactions;● Telemarketing, mail-order, or internet merchants metrics;● Products sold for future delivery, e.g. travel agents and health clubs;● Volume of disputes; and● Chargeback volumes.

<p>17. Determine whether merchant reserve accounts are separately maintained (not commingled with related operating accounts or other merchant reserve accounts).</p> <p><i>Note: Commingling accounts can disguise insufficient reserve levels as it makes it difficult to ensure management is not using the cash flow generated from one merchant to cover the remittance requirement of another merchant.</i></p>
<p>18. Review the composition of merchant customers for concentrations of industries, geographic areas, or other factors.</p> <p><i>Note: Segmenting merchants according to location or activity can help identify concentration risks.</i></p>
<p>19. Ensure procedures are in place to appropriately monitor the financial condition of merchants that present higher risks.</p>
<p>20. Evaluate the bank's pricing system. Pricing policies and practices should ensure that merchants are priced appropriately throughout the life of the contract. Consider the following:</p> <ul style="list-style-type: none">• Minimum discount rates should reflect:<ul style="list-style-type: none">○ The merchant's volume of sales activity,○ Inherent risk in operations, and○ Overall financial conditions.• Management's evaluation of:<ul style="list-style-type: none">○ Employee and equipment costs,○ Cost of float in the clearing process,○ Insurance and bonding needs,○ Loss histories and the risk of future loss,○ Annual budget and strategic plans, and○ Competition.
<p>21. Determine whether management verifies actual sales volumes and ticket sizes to ensure consistency with projected volumes and sizes, at least annually.</p>
<p>22. Evaluate management's compliance with internal risk limits related to capital held to support merchant processing and determine whether the level is appropriate.</p>

23. Determine whether additional capital is needed to support the level of merchant processing. *(Note: No specific capital requirements exist for merchant processing activities; however, examiners should determine whether management periodically assesses the adequacy of capital support relating to credit card related risks. FDIC: Refer to the Credit Card Activities Manual, Chapter XIX, Merchant Processing.)*

Settlement Process

24. Review the vendor management program to ensure management periodically evaluates third-party contingency plans. Assess a sample of contingency plans for parties involved in the settlement process and agents involved in merchant servicing tasks.
Note: When practical, coordinate the vendor management review with Information Technology examiners.

25. Review the settlement process to determine the flow of funds, the parties involved, and who controls funding and settlement.

26. Review a sample of contracts and assess the financial liability of all parties.

27. Determine whether MIS reports provide accurate, timely, and sufficient information for management to assess the function’s activities and results.

28. Determine whether outstanding items in the settlement account clear in a timely fashion.

Chargeback Processing and Reserves

- 29. Assess the adequacy of chargeback monitoring procedures:**
- **Determine whether the bank generates chargeback reports.**
 - **Evaluate the adequacy of the chargeback system. Determine whether the system can perform the following tasks:**
 - **Quantify outstanding chargebacks,**
 - **Identify the age of the chargebacks,**
 - **Prioritize the chargeback research process, and**
 - **Measure the efficiency of the chargeback process.**

- Review significant trends in volume (dollar and number of accounts) and aging of chargebacks.
 - Determine whether the bank’s risk management systems sufficiently track excessive chargebacks.
- Note: The acquiring bank should not place undue reliance on the Association to identify merchants with excessive chargebacks.*

30. Assess the institution's chargeoff policy for stale chargebacks. Classify stale chargebacks according to the FFIEC Uniform Retail Credit Classification and Account Management Policy.

- 31. Determine whether the bank establishes and periodically reviews the adequacy of its chargeback systems and reserves. Consider whether:**
- Management adequately plans for contingencies, such as a large merchant bankruptcy where a material volume of chargebacks occurred;
 - Any significant losses incurred by the bank related to merchant chargebacks;
 - The methodology for establishing required chargeback reserves is adequate;
 - The bank establishes specific merchant reserves or holdback reserves for higher-risk merchants.
 - Reserve deficiency reports identify all significant exposures; and
 - The bank confirmed that merchants implemented chip technology, and (when applicable) assessed risks that could affect a merchant’s financial condition if a merchant did not implement chip technology. (*Note: Chip cards contain an embedded microchip for enhanced security that creates an individual transaction code when used for in-store payments.*)

32. Assess how management reflects merchant chargeback losses on internal reports.

Note: Management should produce reports that identify, on an individual and aggregate basis, chargebacks attributed to individual merchants. For example: Chargeback 1234 of \$50.00 from Merchant ABC. Merchant ABC: Chargebacks YTD total \$9,000.00.

Independent Service Organizations (ISOs) / Merchant Service Providers (MSP)

ISOs solicit merchants' credit card transactions for an acquiring (clearing) bank. Examiners should only complete this section if the bank uses ISOs.

ISOs have assumed an increased role in retail merchant processing activities and rely heavily on sales commissions to generate business; therefore, examiners should assess the bank’s processes controlling risks at ISOs. For example, ISOs should perform appropriate due diligence and monitoring of the retail merchants that they engage. FDIC: Refer to FIL 44-2008, Guidance for Managing Third-Party Risk.

- 33. Review a sample of ISO contracts and assess compliance with the contracts. In general, the contracts should appropriately address items such as:**
- Financial compensation and payment arrangements;

- Fee structures (fees should generally be tied to performance indicators such as sale volumes, number of merchants, and chargeback activity);
- Required security deposits by the ISO to offset potential merchant losses (security deposits should correlate to the ISO's financial condition, the quality of the merchants it solicits, and the level of sales volume it generates);
- Remedies to protect the bank if the ISO fails to perform as expected;
- Requirements for monetary transactions to be handled directly between the bank and the merchant;
- Prohibitions concerning the ISO's ability to assign the agreement or delegate responsibilities to a third party;
- Criteria for acceptability of merchants;
- Control of future use and solicitation of merchants;
- Allowable use of the name, trade name, and logo of the bank and the ISOs;
- Frequency and means of communication and monitoring of each party;
- Records each party must maintain (contracts should allow institutions access to ISO records);
- Frequency and type of financial statements to be required of the ISO;
- Warranties that all consumer laws are followed;
- Handling and other responsibilities for merchant chargebacks; and
- Onsite inspections by bank employees.

34. Determine whether the acquiring bank permits ISO/MSPs to use the bank's VISA Bank Identification Number (BIN) or MasterCard Interbank Card Association number (ICA) to acquire merchants and/or settle credit card transactions. *Note: This arrangement is often referred to as rent-a-bin (RAB). The BIN-owner retains the risk of loss as well as responsibility for settlement with the Associations consistent with the contract between the bank and the Association.*

- Assess management's oversight and control of acquiring RAB arrangements to ensure the ISO/MSP is appropriately managing risks.
- Review any lending relationships the bank has with ISO/MSPs to ensure management analyzes total risk exposures.

35. Review a sample of ISO credit files and assess compliance with policies and guidelines. The files should contain the following items:

- A current financial statement on the principal(s) and the ISO, which should correlate to the size and complexity of the company;
- Initial onsite inspections of ISOs (and periodically thereafter based on performance) performed by a bank employee;
- Evidence of bank and trade references;
- A credit report on the principal(s) of the ISO; and
- A criminal check on the principal(s) of the ISO.

<p>36. Review management's analysis of the financial stability of ISOs, and determine whether ISO reserve accounts are consistent with the condition of the company and the volume of business generated.</p>
<p>37. Review and assess the procedures for monitoring the activities of the ISOs and determine whether adequate due diligence is performed. Consider management's reviews of the ISO's:</p> <ul style="list-style-type: none"> • Operational audits; • Past performance for evidence of misleading advertisements or inappropriate activities; and • Sales methods, customer service practices, and overall operations.
<p>38. Determine whether the bank has registered all ISOs with VISA or MasterCard.</p>
<p>39. Determine whether management reviews promotional material used by ISOs and attends sales training sessions for ISO salespersons.</p>
<p>40. Determine whether management appropriately performs initial and periodic due diligence, risk assessments, and vendor reviews of all ISO's with access to the bank's data systems. <i>Note: Coordinate assessments with Information Technology examiners.</i></p>
<p>41. If the ISO is performing servicing tasks, determine whether management requires an audit of the ISO's technology system.</p>
<p>42. Determine whether contingency plans exist to cover the accounting and servicing functions performed by ISOs to ensure data continuity.</p>
<p>Fraud Detection</p>
<p>43. Review the bank's fraud detection system and determine whether the scope and frequency of the fraud review is adequate. The primary tool of a bank's fraud detection system is the exception report, which is generated from parameters based on expected merchant activities. Fraud identification should not rely exclusively on unusual chargeback activity. A good fraud report should tailor exception parameters for each merchant (beginning with dollar volume of sales and customer chargebacks) and identify the following items:</p>

- Variances in average ticket size,
- Variances in daily volume,
- Multiple same-dollar amounts on tickets,
- Chipped, keyed, and swiped transactions,
- Multiple use of same cardholder number, and
- Inactive merchant accounts.

Note: Exception reports listing merchant's out-of-parameter items should be generated and reviewed daily. Associations and sponsoring banks may also provide educational materials and provide fraudulent activity reports. Fraud monitoring or reports provided by Associations or sponsoring banks should supplement - not replace - the bank's own fraud system.

44. Assess the adequacy of actions taken if suspicious activity is detected. Consider:

- Suspicious Activity Report guidelines,
- Placement of the merchant on MATCH,
- Termination of fraudulent merchant accounts, and
- Other actions taken to suspend or block settlement and/or authorization processing.

Agent Banks

Note: Acquiring (clearing) banks often process credit card transactions for other banks, which are known as agent banks. Depending on the contractual arrangement, the agent bank may or may not be liable to the acquiring bank for chargeback or fraud losses. Only review this section if agent bank relationships exist.

45. Determine whether the bank has an agent bank policy that addresses the following items:

- Agent bank agreements, which should outline the agent bank's financial liability for merchant losses;
- Agent bank merchant underwriting standards, which should be similar to subject bank;
- Approval of policy exceptions;
- Agent bank liabilities and responsibilities regarding merchant fraud;
- Early termination of the agent bank relationship; and
- Approval authorities for each agent bank.

Note: If the agent bank relationship involves only one or two agent banks with minimal activities, formal written policies may not be necessary as long as sound controls exist.

46. Review reports that show agent bank merchant volume by agent bank. Review the activities of agent banks that have significant merchant volume in comparison to the size of the agent bank. (Small banks with large merchant volume may have difficulty fulfilling their responsibilities regarding chargebacks.)

<p>47. Review a sample of agent bank files, if necessary. Evaluate information and check for compliance with internal policy requirements (such as obtaining and reviewing periodic financial information).</p>
<p>Information and Communication Systems</p>
<p>48. Determine whether internal management reports provide sufficient information for risk management decisions and for monitoring the results of those decisions. Reports should provide sufficient detail for the board and senior management to:</p> <ul style="list-style-type: none"> • Identify and monitor risks and their effect on earnings and capital; • Evaluate profitability; and • Verify compliance with risk limits and policy guidelines, including policy exception reporting.
<p>49. Determine whether merchant risks are effectively communicated to all areas affected.</p>
<p>50. Consider testing reports for accuracy by comparing them to regulatory reports and/or subsidiary records.</p>
<p>Board and Senior Management Oversight</p>
<p>51. Determine whether the board provides adequate management resources by (as appropriate):</p> <ul style="list-style-type: none"> • Conducting interviews to determine whether the staff’s technical expertise is commensurate with the scope of operations, • Assessing whether current staffing levels are appropriate for present and future growth plans, and • Determining whether training and development programs are adequate.
<p>52. Determine whether management's plans for the department are clear and communicated to the staff.</p>
<p>53. Review the blanket bond to ensure merchant processing activities have sufficient coverage. <i>Note: Servicers are typically not covered under a bank's fidelity coverage.</i></p>
<p>54. Review the department's operating statements. Compare the statement to the budget and investigate</p>

Core Analysis

significant variances.

End of Core Analysis. If needed, Continue to the Expanded and Impact Analyses.