

<b>CREDIT CARD RELATED MERCHANT ACTIVITIES</b>
--

<b>Core Analysis Decision Factors</b>
---------------------------------------

*Examiners should evaluate the Core Analysis to determine whether an 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 #4-6](#).**

**C.3. Are the audit or independent review functions adequate? Refer to Core Analysis [Procedures #7-8](#).**

**C.4. Are controls over merchants, agent banks, and Independent Sales Organizations (ISOs) adequate? Refer to Core Analysis [Procedures #9-38](#).**

**C.5. Does management properly monitor and control chargebacks, including maintaining adequate reserves for chargebacks? Refer to Core Analysis [Procedures #18-23](#).**

**C.6. Are information and communication systems adequate and accurate? Refer to Core Analysis [Procedures #39-40](#).**

**C.7. Do the board and management effectively supervise this area? Refer to Core Analysis [Procedures #41-47](#).**

## CREDIT CARD RELATED MERCHANT ACTIVITIES

### Core Analysis Procedures

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

#### References

- Third Party Risk - Guidance for Managing Third-Party Risk (FDIC: [FIL 44-2008](#))
- ~~Guidance on Managing Outsourcing Risk (FRB: [SR 13-19 / CA 13-21](#))~~
- ~~FDIC: Credit Card Activities Manual, Chapter XIX, Merchant Processing~~

#### Preliminary Review

##### 1. Review the following items:

- Previous examination reports and workpapers, including actions taken by management to address recommendations
- Recent internal and external audit reports, management letters, and management's response to criticisms or recommendations
- Association correspondence (e.g., Visa and Mastercard)
- Internal memoranda, board minutes, and applicable committee minutes
- Strategic plan and budget
- Management reports to gain a basic understanding of the credit card related merchant activity, such as:
  - Profitability, including trends in the volume of merchant chargebacks and unreconciled items in the settlement account
  - Dollar volume and number of merchants
  - Whether activity primarily accommodates existing customers
  - Merchant risk profiles
  - Concentrations of industries, geographic areas, or other factors<sup>1</sup>
- Management identification of Merchant Service Providers (MSRs) and ISOs used
- Contingent liabilities arising from the bank's processing activities

#### Policies and Procedures

- ##### 2. Determine whether merchant processing policies provide clear and measurable underwriting standards and administrative procedures for merchants. Policies may, but are not required to, include the following:
- Lines of authority and responsibility
  - Risk-assessment and fraud-detection procedures

<sup>1</sup> Segmenting merchants according to location or activity can help identify concentration risks.

<ul style="list-style-type: none"> <li>• Cardholder information security standards</li> <li>• Risk identification practices and limits on the amount of risk the bank is willing to accept</li> <li>• Limits on individual and aggregate volumes or concentrations of merchant activity<sup>2</sup></li> <li>• Requirements for written contracts between all third parties, including reviews of all contracts and applications by legal counsel familiar with merchant processing</li> <li>• Due-diligence criteria for initially accepting, and periodically reviewing: <ul style="list-style-type: none"> <li>○ Merchants' creditworthiness</li> <li>○ Third party compliance with association requirements<sup>3</sup></li> </ul> </li> <li>• Guidelines for monitoring merchant activities and assessing their information-security practices</li> <li>• Criteria for determining the appropriateness of merchant reserve accounts</li> <li>• Criteria for contracting with any ISO to act as agent for the bank</li> <li>• Guidelines for acquiring or issuing rent-a-bins</li> <li>• Guidelines for handling policy exceptions</li> <li>• Guidelines for accepting agent banks</li> <li>• Pricing policies</li> <li>• Markets, merchant types, and risk levels the bank is and is not willing to accept<sup>4</sup></li> <li>• Charge-off policy for stale chargebacks</li> </ul>
<p>3. Determine whether the merchant-processing procedures manual appropriately provides for:</p> <ul style="list-style-type: none"> <li>• Establishing new business relationships</li> <li>• Monitoring existing relationships for credit and financial exposures</li> <li>• Monitoring potential or existing concentrations<sup>5</sup></li> <li>• Working with ISOs</li> <li>• Handling complaints from merchants</li> <li>• Performing settlement procedures that include clearing items in a timely fashion</li> <li>• Processing merchant chargebacks</li> <li>• Training new and existing personnel</li> </ul>
<p><b>Internal Controls</b></p> <p>4. Review recent risk assessments relating to merchant risk profiles and determine whether internal and external threats are identified and mitigated by appropriate controls. Consider whether management uses appropriate risk rating processes (using internal metrics or industry codes).</p>

<sup>2</sup> E.g., limits on the amount of sales volume processed that correlates with merchants' risk profiles.

<sup>3</sup> Such as registration, contract provisions, and audit accessibility.

<sup>4</sup> Characteristics that banks consider when determining restrictions may include business plans, types of merchandise or services offered, and marketing practices. Restrictions may also include order, shipping, and return policies.

<sup>5</sup> E.g., by merchant type or industry, geographic location, or processing volumes by one merchant

<b>5. Determine whether appropriate separation of duties or other compensating controls exist.<sup>6</sup></b>
<b>6. Determine whether appropriate procedures exist to prevent, detect, and respond to policy and procedural exceptions.</b>
<b>Audit or Independent Review<sup>7</sup></b>
<b>7. Determine whether the board and management regularly review audit reports and Association correspondence and appropriately respond to audit findings and Association concerns.</b>
<b>8. Assess the scope, frequency, and effectiveness of the audit program given the risks identified, and determine whether all merchant processing areas are addressed.<sup>8</sup></b>
<b>Merchant Underwriting Standards and Monitoring Procedures</b>
<b>9. Review a sample of files for recently approved merchants including, when applicable, merchants solicited directly by the bank, through ISOs, and through agent banks. Verify that standards are maintained and consider whether files contain the following items:</b> <ul style="list-style-type: none"> <li>• Merchant approval, per policy, ensuring exceptions are appropriately documented</li> <li>• Merchant applications listing the type of business, location, principal(s), and other relevant structure information</li> <li>• Merchant processing agreements that detail all pertinent activities</li> <li>• Merchant risk rating</li> <li>• Corporate resolutions, if applicable</li> <li>• On-site inspection reports</li> <li>• A credit bureau report on the principal(s) of the business</li> <li>• Documented review of prospective merchants against the Member Alert to Control High Risk Merchants (MATCH) system</li> <li>• Financial information on the business (typically received annually)</li> <li>• Merchant tax ID number</li> <li>• Evidence of review of previous merchant activity (recent monthly statements from the previous processor)<sup>9</sup></li> <li>• Estimate of the merchant's projected sales activity and maximum ticket size</li> </ul>

<sup>6</sup> E.g., in the preparation of input and reconciliation of output; for merchant acquisitions and approvals.

<sup>7</sup> Coordinate with examiner completing Audit review.

<sup>8</sup> Effective audit programs will generally: 1) identify contraventions of internal policy, Association regulations, and written contracts, and 2) ensure timely settlement balancing.

<sup>9</sup> Verify that management determines why a merchant has or is switching banks (could indicate excessive chargebacks with previous processor).

<b>10. Determine whether merchant applications are reviewed by a person who has appropriate credit experience.</b>
<b>11. Determine whether underwriting activities and monitoring procedures include information, such as:</b> <ul style="list-style-type: none"> <li>• Projected sales volumes and product delivery periods compared to actual</li> <li>• Projected ticket sizes compared to actual</li> <li>• Card-not-present transactions</li> <li>• Telemarketing, mail-order, or internet merchants metrics</li> <li>• Products sold for future delivery (e.g. travel agents, health clubs)</li> <li>• Volume of disputes</li> <li>• Chargeback volumes</li> </ul>
<b>12. Assess procedures to monitor the financial condition of all merchants, particularly those that present elevated risks.</b>
<b>13. Evaluate the bank's pricing system. Effective pricing policies and practices generally ensure that merchants are priced appropriately throughout the life of the contract. Consider the following:</b> <ul style="list-style-type: none"> <li>• Minimum discount rates generally reflect: <ul style="list-style-type: none"> <li>○ The merchant's volume of sales activity</li> <li>○ Inherent risk in operations</li> <li>○ Overall financial conditions</li> </ul> </li> <li>• Management's evaluation of: <ul style="list-style-type: none"> <li>○ Employee and equipment costs</li> <li>○ Cost of float in the clearing process</li> <li>○ Insurance and bonding needs</li> <li>○ Loss histories and the risk of future loss</li> <li>○ Annual budget and strategic plans</li> <li>○ Competition</li> </ul> </li> </ul>
<b>Settlement Process</b>
<b>14. Review the settlement process to determine the flow of funds, the parties involved, and who controls funding and settlement.</b>

<b>15. Review a sample of contracts and assess the financial liability of all parties.</b>
<b>16. Determine whether outstanding items in the settlement account clear timely.</b>
<b>17. Review the vendor management program to determine whether 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.<sup>10</sup></b>
<b>Chargeback Processing and Reserves<sup>11</sup></b>
<b>18. Determine whether management establishes and periodically assesses its chargeback systems and reserves. Consider whether:</b> <ul style="list-style-type: none"> <li>• Management appropriately plans for contingencies<sup>12</sup></li> <li>• Significant losses incurred by the bank relate to merchant chargebacks</li> <li>• The methodology for establishing required chargeback reserves is adequate</li> <li>• Management establishes specific merchant reserves or holdback reserves for higher risk merchants</li> <li>• Reserve deficiency reports identify all significant exposures</li> <li>• Management 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<sup>13</sup></li> </ul>
<b>19. Evaluate the chargeback system. Determine whether the system can perform the following tasks:</b> <ul style="list-style-type: none"> <li>• Quantify outstanding chargebacks</li> <li>• Identify the age of the chargebacks</li> <li>• Prioritize the chargeback research process</li> <li>• Measure the efficiency of the chargeback process</li> </ul>
<b>20. Select a sample of merchant reserve accounts.</b> <ul style="list-style-type: none"> <li>• Review for compliance with merchant contracts and Association requirements.</li> </ul>

<sup>10</sup> When practical, coordinate the vendor management review with Information Technology examiners.

<sup>11</sup> Effective risk management practices employ chargeback due diligence, and do not unduly rely on the Association to identify merchants with excessive chargebacks.

<sup>12</sup> Such as a large merchant bankruptcy where a material volume of chargebacks occurred.

<sup>13</sup> Chip cards contain an embedded microchip for enhanced security that creates an individual transaction code when used for in-store payments.

<ul style="list-style-type: none"> <li>Determine whether merchant reserve accounts are separately maintained (i.e., not commingled with related operating accounts or other merchant reserve accounts).<sup>14</sup></li> </ul>
21. Review significant trends in volume (dollar and number of accounts) and aging of chargebacks.
22. Assess how management reflects merchant chargeback losses on internal reports. <sup>15</sup>
23. Classify stale chargebacks in accordance with agency policy.
<b>Independent Service Organizations<sup>16</sup> / Merchant Service Providers</b>
<p>24. Review a sample of ISO contracts and assess compliance with the contracts. Contracts generally address items such as:</p> <ul style="list-style-type: none"> <li>Financial compensation and payment arrangements</li> <li>Fee structures<sup>17</sup></li> <li>Required security deposits by the ISO to offset potential merchant losses<sup>18</sup></li> <li>Remedies to protect the bank if the ISO fails to perform as expected</li> <li>Requirements for monetary transactions to be handled directly between the bank and the merchant</li> <li>Prohibitions concerning the ISO's ability to assign the agreement or delegate responsibilities to a third party</li> <li>Criteria for acceptability of merchants</li> <li>Control of future use and solicitation of merchants</li> <li>Allowable use of the name, trade name, and logo of the bank and the ISOs</li> <li>Frequency and means of communication and monitoring of each party</li> <li>Records each party must maintain<sup>19</sup></li> <li>Frequency and type of financial statements required of the ISO</li> <li>Warranties that all consumer laws are followed</li> </ul>

<sup>14</sup> 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.

<sup>15</sup> Reports generally identify, individually and in aggregate, chargebacks attributed to individual merchants.

<sup>16</sup> ISOs have assumed an increased role in retail merchant processing activities and rely heavily on sales commissions to generate business. Effective risk management processes typically involve ISOs performing due diligence and monitoring of the retail merchants that they engage.

<sup>17</sup> Fees generally are tied to performance indicators such as sale volumes, number of merchants, and chargeback activity.

<sup>18</sup> Security deposits generally correlate to the ISO's financial condition, the quality of the merchants it solicits, and the level of sales volume it generates.

<sup>19</sup> Contracts generally allow banks access to ISO records.

<ul style="list-style-type: none"> <li>• <b>Handling and other responsibilities for merchant chargebacks</b></li> <li>• <b>On-site inspections by bank employees</b></li> </ul>
<p><b>25. Determine whether the acquiring bank permits ISOs/MSPs to use the bank's Visa Bank Identification Number (BIN) or MasterCard Interbank Card Association number (ICA) to acquire merchants or settle credit card transactions.<sup>20</sup></b></p> <ul style="list-style-type: none"> <li>• <b>Assess management's oversight and control of acquiring rent-a-bin (RAB) arrangements to determine whether the ISO/MSP is appropriately managing risks</b></li> <li>• <b>Review lending relationships the bank has with ISOs/MSPs to determine whether management analyzes total risk exposures</b></li> </ul>
<p><b>26. Review a sample of ISO credit files and assess compliance with bank policies and guidelines. The files generally contain the following items:</b></p> <ul style="list-style-type: none"> <li>• <b>Current financial statements on the principal(s) and the ISO that correlate to the size and complexity of the company</b></li> <li>• <b>Initial on-site inspections of ISOs (and periodically thereafter based on performance) performed by a bank employee</b></li> <li>• <b>Evidence of bank and trade references</b></li> <li>• <b>A credit report on the principal(s) of the ISO</b></li> <li>• <b>A criminal check on the principal(s) of the ISO</b></li> </ul>
<p><b>27. 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.</b></p>
<p><b>28. 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:</b></p> <ul style="list-style-type: none"> <li>• <b>Operational audits</b></li> <li>• <b>Past performance for evidence of misleading advertisements or inappropriate activities</b></li> <li>• <b>Sales methods, customer service practices, and overall operations</b></li> </ul>
<p><b>29. Determine whether management has registered all ISOs with Visa or MasterCard.</b></p>

<sup>20</sup> This arrangement is often referred to as rent-a-bin. 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.



<b>30. Determine whether management reviews promotional material used by ISOs and attends sales training sessions for ISO salespersons.</b>
<b>31. 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.<sup>21</sup></b>
<b>32. If the ISO performs servicing tasks, determine whether management requires an audit of the ISO's technology system.</b>
<b>33. Determine whether contingency plans exist to cover the accounting and servicing functions performed by ISOs to ensure data continuity.</b>
<b>Fraud Detection</b>
<b>34. 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 fraud detection system is the exception report,<sup>22</sup> which is generated from parameters based on expected merchant activities. Fraud identification should not rely exclusively on unusual chargeback activity. A good fraud report generally tailors exception parameters for each merchant (beginning with dollar volume of sales and customer chargebacks) and identifies items such as the following:</b> <ul style="list-style-type: none"> <li>• Variances in average ticket size</li> <li>• Variances in daily volume</li> <li>• Multiple same-dollar amounts on tickets</li> <li>• Chipped, keyed, and swiped transactions</li> <li>• Multiple use of same cardholder number</li> <li>• Inactive merchant accounts</li> </ul>
<b>35. Assess actions taken by management if suspicious activity is detected. Consider:</b> <ul style="list-style-type: none"> <li>• Suspicious Activity Report guidelines</li> <li>• Placement of the merchant on MATCH</li> <li>• Termination of fraudulent merchant accounts</li> </ul>

<sup>21</sup> Coordinate assessments with Information Technology examiners.

<sup>22</sup> Exception reports listing merchant's out-of-parameter items are generally 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 generally supplement but do not replace the bank's own fraud system.

- Other actions taken to suspend or block settlement or authorization processing

### Agent Banks<sup>23</sup>

**36. Determine whether the bank has an agent bank policy that addresses items such as the following:<sup>24</sup>**

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

**37. Review reports that show 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.<sup>25</sup>**

**38. 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.**

### Information and Communication Systems

**39. Determine whether internal management reports provide sufficient information for risk management decisions and for monitoring the results of those decisions.<sup>26</sup> Reports generally provide sufficient detail for the board and senior management to:**

- Identify and monitor risks and their effect on earnings and capital
- Evaluate the program's profitability
- Verify compliance with risk limits and bank policy guidelines, including policy exception tracking and reporting

**40. Consider testing reports for accuracy by comparing them to regulatory reports and subsidiary records.**

<sup>23</sup> 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.

<sup>24</sup> 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.

<sup>25</sup> Small banks with large merchant volume may have difficulty fulfilling their responsibilities regarding chargebacks.

<sup>26</sup> Consider settlement procedures, and chargeback processing and reserves.

<b>Board and Senior Management Oversight</b>
<b>41. Determine whether the board and senior management regularly review pertinent merchant activity, the program's overall profitability, actual performance versus budget, and overall strategic planning.<sup>27</sup></b>
<b>42. Evaluate management's compliance with internal risk limits related to capital held to support merchant processing.</b>
<b>43. Determine whether management periodically assesses capital support relating to credit card related risks.<sup>28</sup></b>
<b>44. Determine whether the board provides adequate management resources, as appropriate, by:</b> <ul style="list-style-type: none"> <li>• Conducting interviews to determine whether the staff's technical expertise is commensurate with the scope of operations</li> <li>• Assessing whether current staffing levels are appropriate for present and future growth plans</li> <li>• Determining whether training and development programs are adequate</li> </ul>
<b>45. Determine whether management's plans for the department are clear and communicated to the staff.</b>
<b>46. Determine whether merchant risks are effectively communicated to all areas affected.</b>
<b>47. Review the blanket bond to ensure merchant processing activities have sufficient coverage.<sup>29</sup></b>

<sup>27</sup> Information is typically provided using reports, dashboards, or other mechanisms that clearly display the types of merchants they serve and the risks involved, including whether the merchants are generally swipe, keyed, or chip merchants.

<sup>28</sup> No specific capital requirements exist for merchant processing activities. FDIC: Refer to the Credit Card Activities Manual, Chapter XIX, Merchant Processing for capital adequacy considerations.

<sup>29</sup> Servicers are typically not covered under a bank's fidelity coverage. Coordinate with the examiner in the Operations Manager role.

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