XX. THIRD-PARTY RELATIONSHIPS

Banks are increasingly looking to third parties as a way to gain a competitive edge, enhance product offerings, and reduce costs. Effective use of third-party relationships also allows banks to diversify assets and revenues, access greater expertise, and devote human resources that are in short supply to core businesses. However, third-party relationships or vendor management issues can significantly increase a bank's risk profile. As such, the use of third parties for credit card operations has and will continue to receive substantial and increasing regulatory attention.

Banks primarily use third parties in their credit card programs in two ways: to franchise the bank's attributes and to perform functions on the bank's behalf. In the first, the bank lends its name (and thus, regulated entity status) to credit card products, services, and activities that are usually predominantly conducted by others. Franchising arrangements can expose the bank to substantial financial loss and damage to its reputation if it fails to maintain adequate oversight over the third party as well as sufficient quality and other controls over the products and services offered through the third parties. Situations in which the products or services offered are accompanied by fees, interest rates, or other terms that cannot be offered by the third party directly warrant close attention. An issuing Rent-a-BIN arrangement is an example of a franchising situation and is discussed in the Credit Card Issuing Rent-a-BINs chapter. While co-branding, affinity, and similar programs are not predominantly conducted by the third party, they can be thought to be of a franchising nature in that they are operated as a business line carrying the bank's name. Brief comments on these types of arrangements are found later in this chapter.

The majority of this chapter, however, focuses on the second type of third-party use, commonly referred to as outsourcing. Outsourcing covers a wide variety of arrangements, including, but not limited to, core information and transaction processing, collections, marketing, and customer call centers. Several of the concepts for managing outsourcing arrangements mirror concepts for managing franchising arrangements.

Whether in a franchising or outsourcing fashion, a bank's use of third parties for credit card program functions does not diminish management's responsibility to ensure that the activities are conducted in a safe and sound manner as well as in compliance with applicable laws and guidance. An absence of adequate policies for managing third-party arrangements, including selection and oversight, is normally cause for concern. Examiners should also normally expect to see that management subjects third-party relationships to the same risk-management, security, privacy, and other consumer-protection policies as if the bank conducted the activities directly.

OUTSOURCING

Contracting with third parties for services typically enables a bank to offer its customers enhanced services without incurring the expenses involved in owning the technology, maintaining an adequate level of human resources to effectively carry out the function, and so forth. Banks can outsource many areas of credit card operations, including all or part of any service, process, or system operation. The examination normally includes an assessment of management's practices for ensuring that outsourcing of significant functions is consistent with the bank's strategic plans and for evaluating third-party proposals against well-developed acceptance criteria, all prior to engaging in outsourcing.

The examination incorporates an identification of any instances where management has not provided for a comprehensive risk-management process for governing third-party relationships. Each bank's risk profile is unique and requires a tailored risk-mitigation approach appropriate for the scale of its particular third-party credit card relationships, the materiality of the risks present,

and the ability to manage those risks. Nevertheless, there are certain key components common to well-structured third-party risk-management processes:

- Effective risk assessment and strategic planning to identify the bank's needs and requirements. Management's awareness of the risks associated with outsourcing is a prerequisite to establishing suitable controls over such relationships.
- Proper due diligence to identify and select a third-party.
- Comprehensive, written contracts between the bank and the third party.
- Ongoing oversight of the third party and its activities, including determining whether any changes to the arrangements need to be made or whether the relationship should be discontinued.

Examiners should expect management to:

- Ensure each outsourcing relationship supports the bank's overall requirements and strategic plans.
- Make certain the bank has sufficient expertise to oversee and manage the relationship.
- Evaluate prospective third parties based on the scope and critical nature of service(s) to be outsourced.
- Tailor the third-party monitoring program based on initial and ongoing risk assessments of the outsourced services.
- Notify its primary regulators regarding outsourced relationships, when required.
- Register the third party with the applicable Association(s) when required.

Time and resources that management is expected to devote to managing third-party relationships are based on the risk the particular relationship presents to the bank. For instance, outsourcing a processing function for a small, local credit card portfolio usually requires less oversight than outsourcing processing functions for a large, nationwide program with subprime attributes. Smaller and less complex banks may have less flexibility than larger banks when negotiating for services that meet their specific needs and monitoring the third parties. Regardless, regulators hold each bank responsible for proper oversight of its activities conducted by third parties.

Outsourcing does not reduce the fundamental risks associated with the business lines that use it. For example, risks such as loss of funds, loss of competitive advantage, damaged reputation, and improper disclosure of information persist. Furthermore, the bank remains subject to the possibility of regulatory actions regarding the activities. Because the functions are performed by a third party, the risks may be less obvious than if the functions were conducted inside the bank. Nevertheless, substantial risks and the need for proper controls over those risks exist.

RISK CONSIDERATIONS

As mentioned, risk exists whether the bank performs activities internally or elects to outsource them, and management is responsible for appropriately managing risk in all outsourcing relationships**.** While some risks may be direct, banks normally also assume bilateral, or transitive, risk when they outsource. Bilateral, or transitive, risk refers to when the risk at the third party causes risk to the bank. For example, if a third party is doing processing work for a bank, an operations disruption at the third party could affect the bank's operations. Because different vendors provide different services, risks differ among relationships.

Common risks with third-party arrangements are operational and transactional risks (sometimes interchangeable terms). Such risks may arise from fraud or error as well as from the inability to deliver products or services, maintain a competitive position, or manage information. They exist in each process involved in the delivery of the bank's products or services. For example, many banks rely on data-processing providers for their credit card programs and any extended

interruption or termination of service can disrupt normal operations. However, operational and transactional risks include not only operations and transaction processing (such as data processing), but also areas such as customer service, internal control processes, and capacity and contingency planning. Further, operational and transactional risks can affect other risks such as reputation, strategic, legal, and compliance risks.

A third-party's errors, delays, omissions, and similar events that become public knowledge or directly affect customers can significantly affect the bank's reputation. For example, a third-party's failure to maintain adequate contingency plans and facilities for key processes may impair the bank's ability to provide critical services to its customers. A third-party's use of abusive or problematic marketing or collection techniques can also adversely impact the bank's reputation.

From a strategic perspective, inaccurate information from third parties can cause bank management to make poor strategic decisions. For example, if a third-party improperly represents that it has been effectively collecting receivables, management could make a decision to move more collections activity to that third party or to grow the portfolio. The result of those strategic decisions would be that that bank would be faced with higher credit risk than it believed it would have. Inadequate management experience and expertise can also lead to a lack of understanding and control of key third-party risks.

In addition, outsourced activities that fail to comply with legal or regulatory requirements can subject the bank to a variety of legal and regulatory sanctions. For example, inaccurate or untimely consumer compliance disclosures or unauthorized disclosure of confidential customer information could expose the bank to civil money penalties or litigation. Third parties often agree to comply with banking regulations, but their failure to track regulatory changes could increase compliance risk for the serviced banks. Many of the compliance, legal, and reputation risks arising from third-party arrangements easily translate into safety and soundness risks, similar to what is discussed in the Credit Card Issuing Rent-a-BINs chapter.

Credit risk can also result from third-party relationships. For example, if a bank has outsourced the collections functions for its credit card portfolio, a failure of the third-party collector to employ effective collections efforts could result in continued delinquencies (and thereby potentially strained cash flow and increased liquidity risk) as well as more difficulty eliciting recoveries. Further, a third-party's use of overly liberal collection techniques could inappropriately delay loss, for instance if use of workout programs or re-aging is abused.

The quantity of risk associated with outsourcing depends on the function that is outsourced as well as the third party and its technology, processes, techniques, and materials used. In general, the following items are key considerations when evaluating risk at the inception of an outsourcing decision as well as throughout the arrangement's life:

- Sensitivity of data accessed, protected, or controlled by the third party.
- Volume of transactions, accounts, and receivables.
- Criticality of the outsourced function to the bank's business.
- Strength of the third-party's financial condition.
- Management and employee turnover of the third party.
- The third party's ability to maintain business continuity.
- The third party's capability to provide accurate, relevant, and timely MIS.
- The third party's experience with the function outsourced.
- Reliance on subcontractors.
- Location of the third party, particularly if cross-border (foreign-based third-parties).
- Reliability and security of technology and other resources used.
- Ability to accommodate growth, which should consider outsourcing that the third party may also be providing to other parties in addition to the bank.

Further, third-party environments can foster a hierarchy approach in which the third party provides more attention to its top-volume, top-paying, or other big-name customers. If the bank resides in the lower rungs of the hierarchy, the quality of services received could suffer unless management has put appropriate controls in place.

DUE DILIGENCE

Examiners should determine if management's due diligence processes ensure that the third party meets the bank's needs. Effective due diligence processes normally confirm and assess the following regarding the third party:

- Existence and corporate history.
- Qualifications, backgrounds, and reputations of its principals, including criminal background checks where appropriate.
- References, such as other entities that are using the third party for similar services.
- Financial status.
- Strategy and reputation.
- Service delivery capability, status, and effectiveness.
- Technology and systems architecture.
- Internal control environment, security history, and audit coverage.
- Legal compliance including complaints, litigation, and regulatory actions.
- Reliance on and success in dealing with downstream third parties (that is, subcontractors or when the third party outsources functions to another third party).
- Insurance coverage.
- Comprehensive contingency plans.
- Competent employees as well as a sufficient level of employees and resources.

Seeking out information on intangibles, such as the third party's service philosophies, quality initiatives, and management style, is another critical due diligence element. Concern arises when the third party's culture, values, and business styles do not fit those of the bank.

The depth and formality of due diligence normally varies according to the risk of the prospective outsourced relationship as well as the bank's familiarity with the prospective third party. An appendix of the FFIEC's Outsourcing Technology Services booklet (June 2004) provides considerations when the prospective third party is foreign-based.

CONTRACTS

Examiners should expect a written contract to be present for each third-party relationship, including instances where the third party is affiliated. Because of the importance of the contract, the examination normally includes substantiating whether management:

- Verifies the accuracy of the description of the outsourcing relationship in the contract.
- Ensures the contract is clearly written and contains sufficient detail to define the rights and responsibilities of each party.
- Engages legal counsel to help prepare and review proposed contracts.

Common contract elements include, but are not limited to:

- *Scope of Service* – A description of the rights and responsibilities of the parties involved is a main component of the contract.
- *Performance Standards* - Minimum service or performance level requirements and remedies for failure to meet those standards or requirements are normally identified.

The requirements could become ineffective unless management periodically reviews the standards to ensure they remain consistent with the bank's goals and objectives.

- *Security and Confidentiality* - Security and confidentiality of the bank's resources is critical. A failure of the contract to prohibit the service provider and its agents from using or disclosing the bank's information, except as necessary to or consistent with providing the contracted services, is cause for concern as are situations in which the third party does not report to the bank when security breaches occur, the potential or actual effect of those breaches on the bank, and corrective measures.
- *Audit* - Contract commonly specify the types of audit reports the bank is entitled to receive, audit frequency, any charges for obtaining the audits, and the rights of the bank and its regulatory agencies to obtain the results of the audits in a timely manner. It may also specify rights to obtain documentation of the resolution of any deficiencies and to inspect the facilities and operating practices of the third party.
- *Reports* - The frequency and type of reports (for instance, performance reports and financial statements) that will be provided to the bank are normally specified.
- *Business Resumption and Contingency Plans* – Contract provisions normally address the third-party's responsibilities regarding business resumption and contingency plans. Examiner attention should be drawn to contracts that contain provisions that would excuse the third party from implementing its contingency plans.
- *Sub-Contracting* - Some third parties may contract with other third parties. Examiner attention should be directed to instances where management is not aware of and has not approved subcontractors involved in the bank's credit card program. Notification and approval requirements regarding changes to the third-party's significant subcontractors may be defined in the contract.
- *Pricing* – A full description of the compensation method is normally incorporated. Banks usually have many choices for pricing an outsourcing venture. Examples of different pricing methods include cost plus, fixed price, unit pricing, variable pricing, and incentive-based pricing. Contracts also normally specify guidelines for pricing changes in the future. Pricing that appears excessive in relation to the services provided should be closely inspected.
- *Indemnification* – Most contracts include indemnification provisions that require the third party to hold the bank harmless from liability for the third-party's negligence. The strength of the indemnification in reality is closely tied to the third-party's financial condition, and indemnification provisions are not a substitute for proper risk-management practices.
- *Limitation of Liability* - Some contracts contain clauses that limit the amount of liability that can be incurred by the third party. If the bank considers such a contract, examiners should expect that management has assessed whether the damage limitation bears an adequate relationship to the amount of loss the bank might reasonably experience as a result of the third-party's failure to perform its obligations.
- *Termination* - The timeliness and expense of contract termination provisions are key risk points. The extent and flexibility of termination rights varies depending upon the service outsourced. Examiners should look for considerations such as changes in control, convenience, substantial cost increases, repeated failures to meet service levels, failure to provide critical services, bankruptcy, and company closure.
- *Regulatory Compliance* – Concerns arise when contracts do not include an agreement that the third party and any downstream entities will comply with applicable regulatory guidance and requirements and that the third party will provide regulators with accurate information and timely access based on the type and level of service provided to the bank.

The Associations also have certain contracting expectations for certain third-party arrangements. Examiners may refer to the applicable Association's guidelines when applicable.

Examiners should collect any evidence that management has signed contracts that contain provisions or inducements that may adversely affect the bank. For instance, contract provisions that include prolonged durations, significant increases in costs after the first few years, and/or substantial cancellation penalties could expose the bank to unnecessary risk. In addition, some contracts improperly offer inducements that allow a bank to retain or increase capital by deferring losses on the disposition of assets or avoiding expense recognition. These inducements typically attract banks wanting to mask capital problems.

OVERSIGHT PROGRAM

The degree of oversight and review of outsourced credit card activities depends on how critical the service, process, or system is to the bank. Examiners are tasked with evaluating the bank's oversight program for ensuring third parties deliver the quantity and quality of services required by the contract. To increase monitoring effectiveness, management may periodically rank third-party relationships according to risk to determine which service providers require the greatest level of oversight. Rankings are based on the residual risk of the relationship after analyzing the quantity of risk relative to the controls over those risks. Relationships with higher-risk ratings warrant more frequent and stringent monitoring.

Concern is normally justified when personnel responsible for third-party oversight do not have the necessary expertise to assess the risks and/or do not maintain sufficient documentation of the oversight program. Oversight documentation can be helpful to management when renegotiating contracts and developing contingency planning requirements.

Concern is also normally warranted when management has not incorporated on-going monitoring of the financial condition of the third parties in its oversight program. Effective monitoring usually incorporates management reviewing the financial viability of its third parties no less than annually and reporting the results to the board of directors or a designated committee thereof. However, if the third-party's financial condition is declining or unstable, more frequent financial reviews are often warranted. In addition to annual financial statements, management may also use other forms of information to determine a third party's condition, such as independent auditor reports or information provided by public media (trade magazines, newspapers, and so forth).

Examiners should look for evidence that management has executed its contingency plan if it becomes aware that the third-party's financial condition is unstable or deteriorating. Even if the third party remains in operation, its financial problems may jeopardize the quality of its services and possibly the integrity of the data in its possession. A third-party's failure to provide adequate financial data is normally considered a red flag that there may be serious financial stability issues.

Termination of services due to bankruptcy of the third party can have a devastating effect on the bank's operations, particularly if there is not sufficient advance notice of termination, an effective contingency plan, or adequate access to third-party personnel. In such situations, the bank is put into the position of having to address the situation with little advance notice. While many options might be available, they are frequently costly and may cause harmful operating delays.

CONTINGENCY PLANNING

The bank's contingency plan, normally intended to complement its third-parties' plans, is an essential recovery tool when disruption occurs with minimal advance notice. Concerns arise when the plan does not clearly lay out the specific responsibilities of the parties involved. The supervisory approach includes assessing whether management understands all relevant third-party contingency plans, incorporates those requirements within its own plan, and ensures the third party tests its plan at least annually. If the third party maintains an effective contingency plan, disruption of services may likely be minimal and the contract may remain intact.

With respect to monitoring and maintaining contingency plans, management's duties generally include:

- Regularly reviewing the contingency plans of its third parties to ensure any services considered "mission critical" for the bank could be restored within an acceptable timeframe.
- Reviewing contingency plan testing by the third parties. For critical services, annual or more frequent tests of the contingency plan are expected.

INFORMATION SECURITY / SAFEGUARDING

Examiners will expect that management makes certain that information is adequately protected in outsourcing relationships. Banks have a legal responsibility to ensure third parties take appropriate measures to meet information security and safeguarding guidelines. Appropriate due diligence is usually the first line of defense for ensuring the protection of information and systems. Concerns surface when third parties are given access to the information and systems beyond that necessary to perform the outsourced function.

OUTSOURCING TO FOREIGN SERVICE PROVIDERS

Some banks have outsourcing relationships with third parties located in foreign countries. These arrangements can provide cost, expertise, and other advantages and should be subject to the same due diligence and assessment as domestic relationships. However, foreign outsourcing relationships can result in unique strategic, reputation, credit, liquidity, transactional, geographic, and compliance risks. For instance, foreign third parties that provide transaction processing or customer service could magnify compliance and legal risks. Failures by management to identify, assess, prevent, and control the risks warrant examiner attention. Appendix C of the FFIEC's Outsourcing Technology Services booklet (June 2004) includes an appendix about foreign service providers and the risks encountered in such arrangements. While the booklet is IT-focused, several of its concepts translate to safety and soundness concepts. Additional guidance is housed in FIL-52-2006, *Foreign-Based Third-Party Service Providers: Guidance on Managing Risks in These Outsourcing Relationships.*

OUTSOURCING TO AFFILIATED ENTITIES

When outsourcing to an affiliate is considered, management must assure that the arrangement evidences an arms-length transaction. An arrangement between a bank and an affiliate should be on terms that are substantially the same, or at least as favorable to the bank, as those prevailing at the time for comparable transactions with a non-affiliated third party. The costs and quality of services provided should be commensurate with those of a nonaffiliated provider and the arrangement must comply with regulations governing affiliate transactions.

ASSOCIATION REQUIREMENTS

The Associations mainly communicate with their member banks and expect the member banks to convey necessary information to the third parties. In 2004, the Associations began requiring registration for certain third parties used by the member banks. Examiners should determine whether the bank has registered any of the third parties used with the Associations (or has validated Association-registration of the third parties, as applicable) and should gain an understanding of the services provided and responsibilities under registered arrangements. (Nevertheless, examiners must also understand the facets of any unregistered arrangements, namely those of a material nature).

EXAMINATION AND INVESTIGATION OF UNAFFILIATED THIRD-PARTY SERVICERS[19]

Situations occasionally arise where the safety and soundness of an insured depository institution is materially affected by transactions, contracts, or business arrangements with parties that are not affiliated with the institution. When such situations arise, it is necessary for the FDIC to examine the other side of the transaction. The potential impact of these business relationships on the insured depository institution necessitates a complete understanding of the nature of the transaction and relationship and its effect on the insured institution.

By statute, the FDIC has authority to obtain records of unaffiliated service providers and other counterparties relating to an insured financial institution. Such authority is not unqualified but depends on particular facts and circumstances giving rise to inquiries by the FDIC. Several statutory provisions support this conclusion: Sections 10(b) and 10(c) of the FDI Act; Section 7(c) of the BSC Act; and Sections 3(w)(5) and (6) of the FDI Act. The information that the FDIC can obtain from an unaffiliated service provider or other counterparty is not limited to specific transactions with or relating to the insured depository institution but can extend to the financial books and records of the servicer or entity so long as such documents are needed in furtherance of an examination that relates to the affairs of an insured bank.

It is important that examiners are aware of material transactions, service contracts, or other business arrangements that could have a material affect on an insured bank. If it is concluded that information is needed from an unaffiliated service provider or other counterparty to the bank, then the examiner should consult with the Regional Office. The Regional Office will assist the examiner in determining whether information is needed from an unaffiliated service provider, and if so, in obtaining the appropriate information. Examination authority covering bank service corporations is set out in Section 7 of the BSC Act.

AFFINITY, CO-BRANDING, AND CORPORATE CARD ARRANGEMENTS

Affinity, co-branding, and similar arrangements represent forms of third-party arrangements. Examiner attention for these types of programs is normally directed to instances in which management has failed, prior to entering into such arrangement, to analyze the integrity of the third party, to obtain an independent verification of the legitimacy of that entity, to determine the net income expected from the program, and to ascertain the possible effect of high attrition rates should the third party withdraw its endorsement. Because of the possible effect of high attrition rates, examiners should expect the contract to define the length of the relationship as well as renewal and termination procedures. If the relationship is controlled by the third party, that third party could be free to renegotiate card-issuing agreements and take members elsewhere. Examiner attention is also warranted when management is not performing on-going monitoring of the portfolios and programs in these types of arrangements. Monitoring normally includes performance indicators such as, but not limited to, response rates, approval rates, utilization rates, purchase volume, delinquencies, and charge-offs. Examiners should also determine if management has sufficiently reserved for rebate programs, as discussed in the Capital chapter.

[19] The language in this section is taken from the Risk Management Manual of Examination Policies.

RETAIL PARTNERS

Management's review of the financial strength and reputation of the retail partner prior to entering into an agreement is critical to the success of a retail program. Examiners should direct their attention to situations in which management has failed to:

- Maintain documentation and analysis similar to that performed for the bank's commercial borrowers, including the assessment and monitoring of the company's financial condition.
- Consult with legal counsel.
- Establish a contingency plan to deal with bankruptcies.
- Perform ongoing monitoring of the retail portfolios, including performance and quality indicators such as, but not limited to, response rates, approval rates, utilization rates, purchase volume, delinquencies, and charge-offs.

Management's failure to properly provide for these risk-mitigating measures could elevate asset quality problems arising from the failure of a retail partner.

SUMMARY OF EXAMINATION GOALS – THIRD-PARTY RELATIONSHIPS

Examiners are expected to evaluate the quality of risk-management processes used to manage the bank's third-party relationships. As part of their role, examiners should:

- Review policies regarding third-party relationships.
- Assess the level of risk present in outsourcing arrangements, which may include reviewing management's internal risk-ranking processes or risk assessments.
- Evaluate the overall outsourcing process for appropriateness given the size and complexity of the institution as well as the nature of the credit card programs affected.
- Evaluate the third-party selection process, including determining whether due diligence requirements encompass all material aspects of the prospective relationship.
- Evaluate the contracting process.
- Evaluate the bank's process for on-going monitoring of the relationship.