GUIDANCE FOR MANAGING THIRD-PARTY RISK

Introduction

An institution's board of directors and senior management are ultimately responsible for managing activities conducted through third-party relationships, and identifying and controlling the risks arising from such relationships, to the same extent as if the activity were handled within the institution. This guidance includes a description of potential risks arising from third-party relationships, and provides information on identifying and managing risks associated with financial institutions' business relationships with third parties.[1] This guidance applies to any of an institution's third-party arrangements, and is intended to be used as a resource for implementing a third-party risk management program.

This guidance provides a general framework that boards of directors and senior management may use to provide appropriate oversight and risk management of significant third-party relationships. A third-party relationship should be considered significant if the institution's relationship with the third party is a new relationship or involves implementing new bank activities; the relationship has a material effect on the institution's revenues or expenses; the third party performs critical functions; the third party stores, accesses, transmits, or performs transactions on sensitive customer information; the third party markets bank products or services; the third party provides a product or performs a service involving subprime lending or card payment transactions; or the third party poses risks that could significantly affect earnings or capital.

The FDIC reviews a financial institution's risk management program and the overall effect of its third-party relationships as a component of its normal examination process. As noted, the FDIC evaluates activities conducted through third-party relationships as though the activities were performed by the institution itself. In that regard, it must be noted that while an institution may properly seek to mitigate the risks of third-party relationships through the use of indemnity agreements with third parties, such agreements do not insulate the institution from its ultimate responsibility to conduct banking and related activities in a safe and sound manner and in compliance with law.

Management should consider the principles addressed in this guidance and ensure that appropriate procedures are in place, taking into account the complexity and risk potential for each of its third-party relationships. The precise use of a risk management process is dependent upon the nature of the third-party relationship, the scope and magnitude of the activity, and the risk identified.

Background

Financial institutions generally enter into third-party relationships by outsourcing certain operational functions to a third party or by using a third party to make products and services available that the institution does not originate. Also, financial institutions may enter into arrangements with third parties in which the institution funds certain products originated by a third party. As the financial services industry continues to evolve, some financial institutions are also using third parties for functions that are either new or have traditionally been performed in-

[1] This guidance supplements, but does not replace, previously issued information on third-party risk and is intended to assist in the management of third-party relationships.

house. For purposes of this guidance, the term "third party" is broadly defined to include all entities that have entered into a business relationship with the financial institution, whether the third party is a bank or a nonbank, affiliated or not affiliated, regulated or nonregulated, or domestic or foreign.

The FDIC recognizes that the use of third parties can assist management in attaining strategic objectives by increasing revenues or reducing costs. The use of a third party also commonly serves as a vehicle for management to access greater expertise or efficiency for a particular activity. The decision about whether to use a third party should be considered by an institution's board of directors and management taking into account the circumstances unique to the potential relationship. The use of third parties in no way diminishes the responsibility of the board of directors and management to ensure that the third-party activity is conducted in a safe and sound manner and in compliance with applicable laws, regulations, and internal policies.

This guidance provides a general framework for the implementation of an effective third-party risk management process. This guidance does not supersede previously issued FDIC and interagency guidance on managing third-party risk in the context of specific functions or activities. Also, transactions with affiliated entities remain subject to sections 23A and 23B of the Federal Reserve Act—the specific requirements of which are not addressed here.

This guidance applies to any of an institution's third-party arrangements, and is intended to be used as a resource for implementing a third-party risk management program, including functions and activities not specifically addressed in other guidance. The guidelines should not be considered a set of mandatory procedures, but management should ensure that sufficient procedures and policies are in place to control the risks associated with a particular third-party relationship.

Potential Risks Arising from Third-Party Relationships

There are numerous risks that may arise from a financial institution's use of third parties. Some of the risks are associated with the underlying activity itself, similar to the risks faced by an institution directly conducting the activity. Other potential risks arise from or are heightened by the involvement of a third party. Failure to manage these risks can expose an institution to regulatory action, financial loss, litigation and reputation damage, and may even impair the institution's ability to establish new or service existing customer relationships.

Not all of the following risks will be applicable to every third-party relationship; however, complex or significant arrangements may have definable risks in most areas. The financial institution's board of directors and senior management should understand the nature of these risks in the context of the institution's current or planned use of third parties. The following summary of risks is not considered all-inclusive.

Strategic risk. Strategic risk is the risk arising from adverse business decisions, or the failure to implement appropriate business decisions in a manner that is consistent with the institution's strategic goals. The use of a third party to perform banking functions or to offer products or services that do not help the financial institution achieve corporate strategic goals and provide an adequate return on investment exposes the financial institution to strategic risk.

Reputation risk. Reputation risk is the risk arising from negative public opinion. Third-party relationships that result in dissatisfied customers, interactions not consistent with institution policies, inappropriate recommendations, security breaches resulting in the disclosure of customer information, and violations of law and regulation are all examples that could harm the reputation and standing of the financial institution in the community it serves. Also, any negative publicity involving the third party, whether or not the publicity is related to the institution's use of the third party, could result in reputation risk.

Operational risk. Operational risk is the risk of loss resulting from inadequate or failed internal processes, people, and systems or from external events. Third-party relationships often integrate the internal processes of other organizations with the bank's processes and can increase the overall operational complexity.

Transaction risk. Transaction risk is the risk arising from problems with service or product delivery. A third party's failure to perform as expected by customers or the financial institution due to reasons such as inadequate capacity, technological failure, human error, or fraud, exposes the institution to transaction risk. The lack of an effective business resumption plan and appropriate contingency plans increase transaction risk. Weak control over technology used in the third-party arrangement may result in threats to security and the integrity of systems and resources. These issues could result in unauthorized transactions or the inability to transact business as expected.

Credit risk. Credit risk is the risk that a third party, or any other creditor necessary to the third-party relationship, is unable to meet the terms of the contractual arrangements with the financial institution or to otherwise financially perform as agreed. The basic form of credit risk involves the financial condition of the third party itself. Some contracts provide that the third party ensures some measure of performance related to obligations arising from the relationship, such as loan origination programs. In these circumstances, the financial condition of the third party is a factor in assessing credit risk. Credit risk also arises from the use of third parties that market or originate certain types of loans, solicit and refer customers, conduct underwriting analysis, or set up product programs for the financial institution. Appropriate monitoring of the activity of the third party is necessary to ensure that credit risk is understood and remains within board-approved limits.

Compliance risk. Compliance risk is the risk arising from violations of laws, rules, or regulations, or from noncompliance with internal policies or procedures or with the institution's business standards. This risk exists when the products or activities of a third party are not consistent with governing laws, rules, regulations, policies, or ethical standards. For example, some third parties may engage in product marketing practices that are deceptive in violation of Section 5 of the Federal Trade Commission Act, or lending practices that are discriminatory in violation of the Equal Credit Opportunity Act and the Federal Reserve Board's Regulation B. Additionally, the ability of the third party to maintain the privacy of customer records and to implement an appropriate information security and disclosure program is another compliance concern. Liability could potentially extend to the financial institution when third parties experience security breaches involving customer information in violation of the safeguarding of customer information standards under FDIC and Federal Trade Commission regulations. Compliance risk is exacerbated when an institution has inadequate oversight, monitoring or audit functions.

Other risks. The types of risk introduced by an institution's decision to use a third party cannot be fully assessed without a complete understanding of the resulting arrangement. Therefore, a comprehensive list of potential risks that could be associated with a third-party relationship is not possible. In addition to the risks described above, third-party relationships may also subject the financial institution to liquidity, interest rate, price, foreign currency translation, and country risks.

Risk Management Process

The key to the effective use of a third party in any capacity is for the financial institution's management to appropriately assess, measure, monitor, and control the risks associated with the relationship. While engaging another entity may assist management and the board in achieving strategic goals, such an arrangement reduces management's direct control. Therefore, the use of a third party increases the need for oversight of the process from start to finish. This guidance provides four main elements of an effective third-party risk management process: (1) risk assessment, (2) due diligence in selecting a third party, (3) contract structuring and review, and (4) oversight.

While these four elements apply to any third-party activities, the precise use of this process is dependent upon the nature of the third-party relationship, the scope and magnitude of the activity, and the risks identified. These guidelines are not intended to result in an expansion or a decrease in the use of third parties by financial institutions, but to provide a framework for assessing, measuring, monitoring, and controlling risks associated with third parties. A comprehensive risk management process, which includes management of any third-party relationships, will enable management to ensure that capital is sufficient to support the institution's underlying risk exposures and that the third party is operating in a manner consistent with federal and state laws, rules, and regulations, including those intended to protect consumers.

1. Risk Assessment

Risk assessment is fundamental to the initial decision of whether or not to enter into a third-party relationship. The first step in the risk assessment process should be to ensure that the proposed relationship is consistent with the institution's strategic planning and overall business strategy. Next, management should analyze the benefits, costs, legal aspects, and the potential risks associated with the third party under consideration. Expanded analysis would be warranted if the product or service is a new activity or product for the institution. It is key for management to develop a thorough understanding of what the proposed relationship will accomplish for the institution, and why the use of a third party is in its best interests. A risk/reward analysis should be performed for significant matters, comparing the proposed third-party relationship to other methods of performing the activity or product offering, including the use of other vendors or performing the function in-house. For such matters, the analysis should be considered integral to the bank's overall strategic planning, and should thus be performed by senior management and reviewed by the board or an appropriate committee.

Responsible bank personnel should have the requisite knowledge and skills to adequately perform the analysis. Certain aspects of the risk assessment phase may include the use of internal auditors, compliance officers, technology officers, and legal counsel. This phase should also identify performance criteria, internal controls, reporting needs, and contractual requirements that would be critical to the ongoing assessment and control of specific identified

risks. For example, if the activity involves consumer products and services, the board and management should establish a clear solicitation and origination strategy that allows for an assessment of performance, as well as mid-course corrections. In addition, assessing the best method of providing information security and meeting customer privacy requirements should not be overlooked during this phase.

After completing the general assessment of risks, particularly relative to the institution's overall strategic plan, management should review its ability to provide adequate oversight and management of the proposed third-party relationship on an ongoing basis. While identifying and understanding the risks associated with the third party is critical at the outset, the long-term management of the relationship is vital to success. For significant third-party relationships, the board may consider appointing a senior manager to be responsible for the relationship, including due diligence, implementation, ongoing oversight, and periodic reporting to the board. This management official should have the requisite knowledge and skills to critically review all aspects of the relationship. The board and management should also ensure that the institution's compliance management system is adapted to effectively address the third-party relationship and appropriately respond to emerging issues and compliance deficiencies.

A final part of the initial risk assessment phase for significant relationships involves carefully estimating the long-term financial effect of the proposed third-party relationship. The board should take into account all aspects of the long-term potential of the relationship, as well as the managerial expertise and other associated costs that would result from the decision to use a third party, and not be unduly influenced by short-term cost savings. The long-term financial risk resulting from an initial incomplete accounting of costs and/or an overestimation of benefits can undermine appropriate decisions in other phases of the risk management process.

2. Due Diligence in Selecting a Third Party

Following an assessment of risks and a decision to proceed with a plan to establish a third-party relationship, management must select a qualified entity to implement the activity or program. The due diligence process provides management with the information needed to address qualitative and quantitative aspects of potential third parties to determine if a relationship would help achieve the financial institution's strategic and financial goals and mitigate identified risks. Not only should due diligence be performed prior to selecting a third party, but it should also be performed periodically during the course of the relationship, particularly when considering a renewal of a contract.

The scope and depth of due diligence is directly related to the importance and magnitude of the institution's relationship with the third party. For example, large-scale, highly visible programs or programs dealing with sensitive data integral to the institution's success warrant an in-depth due diligence of the potential third party, while the due diligence process for isolated low-risk third-party activities would be much less comprehensive.

Comprehensive due diligence involves a review of all available information about a potential third party, focusing on the entity's financial condition, its specific relevant experience, its knowledge of applicable laws and regulations, its reputation, and the scope and effectiveness of its operations and controls. The evaluation of a third party may include the following items:

- Audited financial statements, annual reports, SEC filings, and other available financial indicators.
- Significance of the proposed contract on the third party's financial condition.
- Experience and ability in implementing and monitoring the proposed activity.
- Business reputation.
- Qualifications and experience of the company's principals.
- Strategies and goals, including service philosophies, quality initiatives, efficiency improvements, and employment policies.
- Existence of any significant complaints or litigation, or regulatory actions against the company.
- Ability to perform the proposed functions using current systems or the need to make additional investment.
- Use of other parties or subcontractors by the third party.
- Scope of internal controls, systems and data security, privacy protections, and audit coverage.
- Business resumption strategy and contingency plans.
- Knowledge of relevant consumer protection and civil rights laws and regulations.
- Adequacy of management information systems.
- Insurance coverage.

3. Contract Structuring and Review

After selecting a third party, management should ensure that the specific expectations and obligations of both the financial institution and the third party are outlined in a written contract prior to entering into the arrangement. Board approval should be obtained prior to entering into any material third-party arrangements. Appropriate legal counsel should also review significant contracts prior to finalization. Any material or significant contract with a third party should prohibit assignment, transfer or subcontracting by the third party of its obligations to another entity, unless and until the financial institution determines that such assignment, transfer, or subcontract would be consistent with the due diligence standards for selection of third parties.

The level of detail in contract provisions will vary with the scope and risks associated with the third-party relationship. The following topics should be considered as a contract is structured, with the applicability of each dependent upon the nature and significance of the third-party relationship.

Scope. The contract should clearly set forth the rights and responsibilities of each party to the contract, including the following:

- Timeframe covered by the contract.
- Frequency, format, and specifications of the service or product to be provided.
- Other services to be provided by the third party, such as software support and maintenance, training of employees, and customer service.
- Requirement that the third party comply with all applicable laws, regulations, and regulatory guidance.
- Authorization for the institution and the appropriate federal and state regulatory agency to have access to records of the third party as are necessary or appropriate to evaluate compliance with laws, rules, and regulations.

- Identification of which party will be responsible for delivering any required customer disclosures.
- Insurance coverage to be maintained by the third party.
- Terms relating to any use of bank premises, equipment, or employees.
- Permissibility/prohibition of the third party to subcontract or use another party to meet its obligations with respect to the contract, and any notice/approval requirements.
- Authorization for the institution to monitor and periodically review the third party for compliance with its agreement.
- Indemnification.

Cost/compensation. For both the financial institution and the third party, the contract should outline the fees to be paid, including any fixed compensation, variable charges, and any fees to be paid for nonrecurring items or special requests. Other items that should be addressed, if applicable, are the cost and responsibility for purchasing and maintaining any equipment, hardware, software, or other item related to the activity. Also, the party responsible for payment of any legal or audit expenses should be identified.

Financial institutions should employ compensation programs that are consistent with sound banking practices and consumer protection laws. Compensation schemes should be structured to promote favorable long-term performance in a safe and sound manner. Volume and short-term incentives should be subject to strict quality control, and in the area of loan originations, are of particular concern. The FDIC expressly discourages the use of compensation arrangements which may encourage third-party originators to inappropriately steer borrowers into higher cost products.

Performance standards. For certain relationships, clearly defined performance standards should be included to serve as a basis for measuring the performance of the third party, and may also be used as a factor in compensation arrangements. Industry standards may be used as a reference for certain functions, or standards may be set to reflect the particular relationship between the third party and the financial institution. Management should periodically review the performance measures to ensure consistency with its overall objectives.

Reports. The contract should specify the type and frequency of management information reports to be received from the third party. Routine reports may include performance reports, audits, financial reports, security reports, and business resumption testing reports. Management should also consider mandating exception-based reports that would serve as notification of any changes or problems that could affect the nature of the relationship or pose a risk to the financial institution.

Audit. In addition to the types and frequency of audit reports that the financial institution is entitled to receive from the third party, the contract should also specify the institution's right to audit the third party (or engage an independent auditor) as needed to monitor performance under the contract. Management should ensure that the third party's internal control environment as it relates to the service or product being provided to the financial institution is sufficiently audited. If material to the arrangement, specific internal controls to be maintained by the third party should be defined in the contract.

Confidentiality and security. The contract should prohibit the third party and its agents from using or disclosing the institution's information, except as necessary to perform the functions designated by the contract. Any nonpublic personal information on the institution's customers must be handled in a manner consistent with the institution's own privacy policy and in accordance with applicable privacy laws and regulations. Any breaches in the security and confidentiality of information, including a potential breach resulting from an unauthorized intrusion, should be required to be fully and promptly disclosed to the financial institution.

Customer complaints. The contract should specify whether the financial institution or the third party has the duty to respond to any complaints received by the third party from customers of the financial institution. If the third party is responsible for such responses, a copy of any complaint and the response should be forwarded to the financial institution. The contract should also provide for periodic summary reports detailing the status and resolution of complaints.

Business resumption and contingency plans. The contract should address the third party's responsibility for continuation of services provided for in the contractual arrangement in the event of an operational failure, including both man-made and natural disasters. The third party should have appropriate protections for backing up information and also maintain disaster recovery and contingency plans with sufficiently detailed operating procedures. Results of testing of these plans should be provided to the financial institution.

Default and termination. To mitigate risks associated with contract default and/or termination, the contract should address both issues. The contract should specify what circumstances constitute default, identify remedies, and allow for a reasonable opportunity to cure a default. Similarly, termination rights should be identified in the contract, especially for material third-party arrangements and relationships involving rapidly changing technology or circumstances. Termination rights may be sought for various conditions, such as a change in control, substantial increase in cost, failure to meet performance standards, failure to fulfill contractual obligations, inability to prevent violations of law, bankruptcy, company closure, and insolvency. The contract should state termination and notification requirements, with operating requirements and time frames to allow for the orderly conversion to another entity without excessive expense. Return of the financial institution's data, records, and/or other resources should also be addressed.

Dispute resolution. The institution should consider whether the contract should include a dispute resolution process for the purpose of resolving problems expeditiously. Continuation of the arrangement between the parties during the dispute should also be addressed.

Ownership and license. The contract should address ownership issues and the third party's right to use the financial institution's property, including data, equipment, software, and intellectual property such as the institution's name and logo, trademark, and other copyrighted material. It should also address ownership and control of any records generated by the third party.

Indemnification. Indemnification provisions require a third party to hold the financial institution harmless from liability as a result of negligence by the third party, and vice versa. Incorporating these provisions into a contract may reduce the potential for the institution to be held liable for claims arising from the third party's negligence. It bears repeating, however, that such provisions cannot shift to third parties the institution's ultimate responsibility to conduct banking

and related activities in a safe and sound manner and in compliance with laws, regulations and sound banking principles. Also, the existence of indemnification provisions will not be a mitigating factor where deficiencies indicate the need to seek corrective actions. Where violations of consumer protection or other laws, regulations, and sound banking principles are present, or when banking and related activities are not conducted in a safe and sound manner, the FDIC's consideration of remedial measures, including restitution orders, will be made irrespective of the existence of indemnification clauses in third-party contracts.

Limits on liability. A third party may wish to contractually limit the amount of liability that it could incur as a result of the relationship with the financial institution. Before entering into such a contract, management of the financial institution should carefully consider whether the proposed damage limitation is reasonable compared to the amount of loss the institution could experience should the third party fail to adequately perform.

4. Oversight

Institutions should maintain adequate oversight of third-party activities and adequate quality control over those products and services provided through third-party arrangements in order to minimize exposure to potential significant financial loss, reputation damage, and supervisory action. The board should initially approve, oversee, and review at least annually significant third-party arrangements, and review these arrangements and written agreements whenever there is a material change to the program. Management should periodically review the third party's operations in order to verify that they are consistent with the terms of the written agreement and that risks are being controlled. The institution's compliance management system should ensure continuing compliance with applicable federal and state laws, rules, and regulations, as well as internal policies and procedures.

Management should allocate sufficient qualified staff to monitor significant third-party relationships and provide the necessary oversight. Management should consider designating a specific officer to coordinate the oversight activities with respect to significant relationships, and involve their compliance management function and, as necessary, involve other operational areas such as audit and information technology, in the monitoring process. The extent of oversight of a particular third-party relationship will depend upon the potential risks and the scope and magnitude of the arrangement.

An oversight program will generally include monitoring of the third party's quality of service, risk management practices, financial condition, and applicable controls and reports. Results of oversight activities for material third-party arrangements should be periodically reported to the financial institution's board of directors or designated committee. Identified weaknesses should be documented and promptly addressed.

Performance monitoring should include, as appropriate, the following:

- Evaluate the overall effectiveness of the third-party relationship and the consistency of the relationship with the financial institution's strategic goals.
- Review any licensing or registrations to ensure the third party can legally perform its services.
- Evaluate the third party's financial condition at least annually. Financial review should be as comprehensive as the credit risk analysis performed on the institution's borrowing

relationships. Audited financial statements should be required for significant third-party relationships.

- Review the adequacy of the third party's insurance coverage.
- Ensure that the third party's financial obligations to others are being met.
- Review audit reports or other reports of the third party, and follow up on any needed corrective actions.
- Review the adequacy and adherence to the third party's policies relating to internal controls and security issues.
- Monitor for compliance with applicable laws, rules, and regulations.
- Review the third party's business resumption contingency planning and testing.
- Assess the effect of any changes in key third party personnel involved in the relationship with the financial institution.
- Review reports relating to the third party's performance in the context of contractual requirements and performance standards, with appropriate follow-up as needed.
- Determine the adequacy of any training provided to employees of the financial institution and the third party.
- Administer any testing programs for third parties with direct interaction with customers.
- Review customer complaints about the products and services provided by the third party and the resolution of the complaints.
- Meet as needed with representatives of the third party to discuss performance and operational issues.

Proper documentation will facilitate the monitoring and management of the risks associated with third-party relationships. Therefore, institutions should maintain documents and records on all aspects of the third-party relationship, including valid contracts, business plans, risk analyses, due diligence, and oversight activities (including reports to the board or delegated committees). Also, retain documents regarding any dispute resolution.

FDIC Supervision of Third-Party Relationships

A financial institution's board of directors and senior management are responsible for identifying and controlling risks arising from third-party relationships to the same extent as if the third-party activity were handled within the institution. The FDIC reviews a financial institution's management of significant third-party relationships in the context of the normal supervisory process. In addition to safety and soundness examinations, the FDIC compliance examinations evaluate the quality and effectiveness of an institution's compliance risk management program as it pertains to third-party arrangements, and reviews these operations to ensure that the products, services, and activities of a third party comply with consumer protection and civil rights laws and regulations. Further, reviews of third-party arrangements are often a critical area included in examinations of the trust and information technology functions.

The principal focus of supervisory efforts is the review of management's record and process of assessing, measuring, monitoring, and controlling risks associated with an institution's significant third-party relationships. The depth of the examination review will depend upon the scope of activity conducted through or by the third party and the degree of risk associated with the activity and relationship.

Review of third-party relationships contributes to the FDIC's overall evaluation of management and its ability to effectively control risk. Additionally, the use of third parties could have a significant effect on other key aspects of performance, such as earnings, asset quality, liquidity, rate sensitivity, and the institution's ability to comply with laws and regulations. Findings resulting from the review of an institution's third-party relationships will be addressed as needed in the Report of Examination. Appropriate corrective actions, including enforcement actions, may be pursued for deficiencies related to a third-party relationship that pose a safety and soundness or compliance management concern or result in violations of applicable Federal or State laws or regulations. Financial institutions are reminded that indemnity or other contractual provisions with third parties cannot insulate the financial institution from such corrective actions.

Finally, financial institutions should in all cases take care to comply with Section 7 of The Bank Service Company Act (12 U.S.C. 1867) which requires insured financial institutions to notify their appropriate federal banking agency in writing of contracts or relationships with third parties that provide certain services to the institution. These services include check and deposit sorting and posting, computation and posting of interest and other credits and charges, preparation and mailing of checks, statements, notices, and similar items, or any other clerical, bookkeeping, accounting, statistical, or similar functions performed for a depository institution. Refer to Financial Institution Letter 49-99, dated June 3, 1999.