AGENCY VRM GUIDANCE

Federal Deposit Insurance Corporation

Financial Institution Letters

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-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.

---

[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.

Guidance on Managing Outsourcing Risk

Division of Banking Supervision and Regulation
Division of Consumer and Community Affairs
Board of Governors of the Federal Reserve System

December 5, 2013

Table of Contents

I. Purpose

In addition to traditional core bank processing and information technology services, financial institutions[1] outsource operational activities such as accounting, appraisal management, internal audit, human resources, sales and marketing, loan review, asset and wealth management, procurement, and loan servicing. The Federal Reserve is issuing this guidance to financial institutions to highlight the potential risks arising from the use of service providers and to describe the elements of an appropriate service provider risk management program. This guidance supplements existing guidance on technology service provider (TSP) risk,[2] and applies to service provider relationships where business functions or activities are outsourced. For purposes of this guidance, "service providers" is broadly defined to include all entities[3] that have entered into a contractual relationship with a financial institution to provide business functions or activities.

II. Risks from the Use of Service Providers

The use of service providers to perform operational functions presents various risks to financial institutions. Some risks are inherent to the outsourced activity itself, whereas others are introduced with the involvement of a service provider. If not managed effectively, the use of service providers may expose financial institutions to risks that can result in regulatory action, financial loss, litigation, and loss of reputation. Financial institutions should consider the following risks before entering into and while managing outsourcing arrangements.

- *Compliance risks* arise when the services, products, or activities of a service provider fail to comply with applicable U.S. laws and regulations.
- *Concentration risks* arise when outsourced services or products are provided by a limited number of service providers or are concentrated in limited geographic locations.
- *Reputational risks* arise when actions or poor performance of a service provider causes the public to form a negative opinion about a financial institution.

---

[1] For purposes of this guidance, a "financial institution" refers to state member banks, bank and savings and loan holding companies (including their nonbank subsidiaries), and U.S. operations of foreign banking organizations.

[2] Refer to the *FFIEC Outsourcing Technology Services Booklet* (June 2004) at http://ithandbook.ffiec.gov/it-booklets/outsourcing-technology-services.aspx.

[3] Entities may be a bank or nonbank, affiliated or non-affiliated, regulated or non-regulated, or domestic or foreign.

- *Country risks* arise when a financial institution engages a foreign-based service provider, exposing the institution to possible economic, social, and political conditions and events from the country where the provider is located.
- *Operational risks* arise when a service provider exposes a financial institution to losses due to inadequate or failed internal processes or systems or from external events and human error.
- *Legal risks* arise when a service provider exposes a financial institution to legal expenses and possible lawsuits.

III. Board of Directors and Senior Management Responsibilities

The use of service providers does not relieve a financial institution's board of directors and senior management of their responsibility to ensure that outsourced activities are conducted in a safe-and-sound manner and in compliance with applicable laws and regulations. Policies governing the use of service providers should be established and approved by the board of directors, or an executive committee of the board. These policies should establish a service provider risk management program that addresses risk assessments and due diligence, standards for contract provisions and considerations, ongoing monitoring of service providers, and business continuity and contingency planning.

Senior management is responsible for ensuring that board-approved policies for the use of service providers are appropriately executed. This includes overseeing the development and implementation of an appropriate risk management and reporting framework that includes elements described in this guidance. Senior management is also responsible for regularly reporting to the board of directors on adherence to policies governing outsourcing arrangements.

IV. Service Provider Risk Management Programs

A financial institution's service provider risk management program should be risk-focused and provide oversight and controls commensurate with the level of risk presented by the outsourcing arrangements in which the financial institution is engaged. It should focus on outsourced activities that have a substantial impact on a financial institution's financial condition; are critical to the institution's ongoing operations; involve sensitive customer information or new bank products or services; or pose material compliance risk.

The depth and formality of the service provider risk management program will depend on the criticality, complexity, and number of material business activities being outsourced. A

community banking organization may have critical business activities being outsourced, but the number may be few and to highly reputable service providers. Therefore, the risk management program may be simpler and use less elements and considerations. For those financial institutions that may use hundreds or thousands of service providers for numerous business activities that have material risk, the financial institution may find that they need to use many more elements and considerations of a service provider risk management program to manage the higher level of risk and reliance on service providers.

While the activities necessary to implement an effective service provider risk management program can vary based on the scope and nature of a financial institution's outsourced activities, effective programs usually include the following core elements:

A. Risk assessments;

B. Due diligence and selection of service providers;

C. Contract provisions and considerations;

D. Incentive compensation review;

E. Oversight and monitoring of service providers; and

F. Business continuity and contingency plans.

A. Risk Assessments

Risk assessment of a business activity and the implications of performing the activity in-house or having the activity performed by a service provider are fundamental to the decision of whether or not to outsource. A financial institution should determine whether outsourcing an activity is consistent with the strategic direction and overall business strategy of the organization. After that determination is made, a financial institution should analyze the benefits and risks of outsourcing the proposed activity as well as the service provider risk, and determine cost implications for establishing the outsourcing arrangement. Consideration should also be given to the availability of qualified and experienced service providers to perform the service on an ongoing basis. Additionally, management should consider the financial institution's ability and expertise to provide appropriate oversight and management of the relationship with the service provider.

This risk assessment should be updated at appropriate intervals consistent with the financial institution's service provider risk management program. A financial institution should revise its risk mitigation plans, if appropriate, based on the results of the updated risk assessment.

B. Due Diligence and Selection of Service Providers

A financial institution should conduct an evaluation of and perform the necessary due diligence for a prospective service provider prior to engaging the service provider. The depth and formality of the due diligence performed will vary depending on the scope, complexity, and

importance of the planned outsourcing arrangement, the financial institution's familiarity with prospective service providers, and the reputation and industry standing of the service provider. Throughout the due diligence process, financial institution technical experts and key stakeholders should be engaged in the review and approval process as needed. The overall due diligence process includes a review of the service provider with regard to:

1. Business background, reputation, and strategy;
2. Financial performance and condition; and
3. Operations and internal controls.

1. Business Background, Reputation, and Strategy

Financial institutions should review a prospective service provider's status in the industry and corporate history and qualifications; review the background and reputation of the service provider and its principals; and ensure that the service provider has an appropriate background check program for its employees.

The service provider's experience in providing the proposed service should be evaluated in order to assess its qualifications and competencies to perform the service. The service provider's business model, including its business strategy and mission, service philosophy, quality initiatives, and organizational policies should be evaluated. Financial institutions should also consider the resiliency and adaptability of the service provider's business model as factors in assessing the future viability of the provider to perform services.

Financial institutions should check the service provider's references to ascertain its performance record, and verify any required licenses and certifications. Financial institutions should also verify whether there are any pending legal or regulatory compliance issues (for example, litigation, regulatory actions, or complaints) that are associated with the prospective service provider and its principals.

2. Financial Performance and Condition

Financial institutions should review the financial condition of the service provider and its closely-related affiliates. The financial review may include:

- The service provider's most recent financial statements and annual report with regard to outstanding commitments, capital strength, liquidity and operating results.
- The service provider's sustainability, including factors such as the length of time that the service provider has been in business and the service provider's growth of market share for a given service.
- The potential impact of the financial institution's business relationship on the service provider's financial condition.

- The service provider's commitment (both in terms of financial and staff resources) to provide the contracted services to the financial institution for the duration of the contract.
- The adequacy of the service provider's insurance coverage.
- The adequacy of the service provider's review of the financial condition of any subcontractors.
- Other current issues the service provider may be facing that could affect future financial performance.

3. Operations and Internal Controls

Financial institutions are responsible for ensuring that services provided by service providers comply with applicable laws and regulations and are consistent with safe-and-sound banking practices. Financial institutions should evaluate the adequacy of standards, policies, and procedures. Depending on the characteristics of the outsourced activity, some or all of the following may need to be reviewed:

- Internal controls;
- Facilities management (such as access requirements or sharing of facilities);
- Training, including compliance training for staff;
- Security of systems (for example, data and equipment);
- Privacy protection of the financial institution's confidential information;
- Maintenance and retention of records;
- Business resumption and contingency planning;
- Systems development and maintenance;
- Service support and delivery;
- Employee background checks; and
- Adherence to applicable laws, regulations, and supervisory guidance.

C. Contract Provisions and Considerations

Financial institutions should understand the service contract and legal issues associated with proposed outsourcing arrangements. The terms of service agreements should be defined in written contracts that have been reviewed by the financial institution's legal counsel prior to execution. The characteristics of the business activity being outsourced and the service

provider's strategy for providing those services will determine the terms of the contract. Elements of well-defined contracts and service agreements usually include:

- ***Scope:*** Contracts should clearly define the rights and responsibilities of each party, including:
  - Support, maintenance, and customer service;
  - Contract timeframes;
  - Compliance with applicable laws, regulations, and regulatory guidance;
  - Training of financial institution employees;
  - The ability to subcontract services;
  - The distribution of any required statements or disclosures to the financial institution's customers;
  - Insurance coverage requirements; and
  - Terms governing the use of the financial institution's property, equipment, and staff.
- ***Cost and compensation:*** Contracts should describe the compensation, variable charges, and any fees to be paid for non-recurring items and special requests. Agreements should also address which party is responsible for the payment of any legal, audit, and examination fees related to the activity being performed by the service provider. Where applicable, agreements should address the party responsible for the expense, purchasing, and maintenance of any equipment, hardware, software or any other item related to the activity being performed by the service provider. In addition, financial institutions should ensure that any incentives (for example, in the form of variable charges, such as fees and/or commissions) provided in contracts do not provide potential incentives to take imprudent risks on behalf of the institution.
- ***Right to audit:*** Agreements may provide for the right of the institution or its representatives to audit the service provider and/or to have access to audit reports. Agreements should define the types of audit reports the financial institution will receive and the frequency of the audits and reports.
- ***Establishment and monitoring of performance standards:*** Agreements should define measurable performance standards for the services or products being provided.
- ***Confidentiality and security of information:*** Consistent with applicable laws, regulations, and supervisory guidance, service providers should ensure the security and confidentiality of both the financial institution's confidential information and the financial institution's customer information. Information security measures for outsourced functions should be viewed as if the activity were being performed by the financial institution and afforded the same protections. Financial institutions have a responsibility to ensure service providers take appropriate measures designed to meet

the objectives of the information security guidelines within Federal Financial Institutions Examination Council (FFIEC) guidance[4], as well as comply with section 501(b) of the Gramm-Leach-Bliley Act. These measures should be mapped directly to the security processes at financial institutions, as well as be included or referenced in agreements between financial institutions and service providers.

Service agreements should also address service provider use of financial institution information and its customer information. Information made available to the service provider should be limited to what is needed to provide the contracted services. Service providers may reveal confidential supervisory information only to the extent authorized under applicable laws and regulations.[5]

If service providers handle any of the financial institution customer's Nonpublic Personal Information (NPPI), the service providers must comply with applicable privacy laws and regulations.[6] Financial institutions should require notification from service providers of any breaches involving the disclosure of NPPI data. Generally, NPPI data is any nonpublic personally identifiable financial information; and any list, description, or other grouping of consumers (and publicly available information pertaining to them) derived using any personally identifiable financial information that is not publicly available.[7] Financial institutions and their service providers who maintain, store, or process NPPI data are responsible for that information and any disclosure of it. The security of, retention of, and access to NPPI data should be addressed in any contracts with service providers.

When a breach or compromise of NPPI data occurs, financial institutions have legal requirements that vary by state and these requirements should be made part of the contracts between the financial institution and any service provider that provides storage, processing, or transmission of NPPI data. Misuse or unauthorized disclosure of confidential customer data by service providers may expose financial institutions to liability or action by a federal or state regulatory agency. Contracts should clearly authorize and disclose the roles and responsibilities of financial institutions and service providers regarding NPPI data.

- ***Ownership and license:*** Agreements should define the ability and circumstances under which service providers may use financial institution property inclusive of data, hardware, software, and intellectual property. Agreements should address the ownership and control of any information generated by service providers. If financial institutions purchase software from service providers, escrow agreements may be

---

[4] For further guidance regarding vendor security practices, refer to the *FFIEC Information Security Booklet* (July 2006) at http://ithandbook.ffiec.gov/it-booklets/information-security.aspx.

[5] *See* 12 CFR Part 261.

[6] *See* 12 CFR Part 1016.

[7] *See* 12 U.S.C. 6801(b).

needed to ensure that financial institutions have the ability to access the source code and programs under certain conditions.[8]

- ***Indemnification:*** Agreements should provide for service provider indemnification of financial institutions for any claims against financial institutions resulting from the service provider's negligence.

- ***Default and termination:*** Agreements should define events of a contractual default, list of acceptable remedies, and provide opportunities for curing default. Agreements should also define termination rights, including change in control, merger or acquisition, increase in fees, failure to meet performance standards, failure to fulfill the contractual obligations, failure to provide required notices, and failure to prevent violations of law, bankruptcy, closure, or insolvency. Contracts should include termination and notification requirements that provide financial institutions with sufficient time to transfer services to another service provider. Agreements should also address a service provider's preservation and timely return of financial institution data, records, and other resources.

- ***Dispute resolution:*** Agreements should include a dispute resolution process in order to expedite problem resolution and address the continuation of the arrangement between the parties during the dispute resolution period.

- ***Limits on liability:*** Service providers may want to contractually limit their liability. The board of directors and senior management of a financial institution should determine whether the proposed limitations are reasonable when compared to the risks to the institution if a service provider fails to perform.[9]

- ***Insurance:*** Service providers should have adequate insurance and provide financial institutions with proof of insurance. Further, service providers should notify financial institutions when there is a material change in their insurance coverage.

- ***Customer complaints:*** Agreements should specify the responsibilities of financial institutions and service providers related to responding to customer complaints. If service providers are responsible for customer complaint resolution, agreements should provide for summary reports to the financial institutions that track the status and resolution of complaints.

- ***Business resumption and contingency plan of the service provider:*** Agreements should address the continuation of services provided by service providers in the event of operational failures. Agreements should address service provider responsibility for

---

[8] Escrow agreements are established with vendors when buying or leasing products that have underlying proprietary software. In such agreements, an organization can only access the source program code under specific conditions, such as discontinued product support or financial insolvency of the vendor.

[9] Refer to SR letter 06-4, "Interagency Advisory on the Unsafe and Unsound Use of Limitations on Liability Provisions in External Audit Engagement Letters," regarding restrictions on the liability limitations for external audit engagements at http://www.federalreserve.gov/boarddocs/srletters/2006/SR0604.htm.

backing up information and maintaining disaster recovery and contingency plans. Agreements may include a service provider's responsibility for testing of plans and providing testing results to financial institutions.

- ***Foreign-based service providers:*** For agreements with foreign-based service providers, financial institutions should consider including express choice of law and jurisdictional provisions that would provide for the adjudication of all disputes between the two parties under the laws of a single, specific jurisdiction. Such agreements may be subject to the interpretation of foreign courts relying on local laws. Foreign law may differ from U.S. law in the enforcement of contracts. As a result, financial institutions should seek legal advice regarding the enforceability of all aspects of proposed contracts with foreign-based service providers and the other legal ramifications of such arrangements.

- ***Subcontracting:*** If agreements allow for subcontracting, the same contractual provisions should apply to the subcontractor. Contract provisions should clearly state that the primary service provider has overall accountability for all services that the service provider and its subcontractors provide. Agreements should define the services that may be subcontracted, the service provider's due diligence process for engaging and monitoring subcontractors, and the notification and approval requirements regarding changes to the service provider's subcontractors. Financial institutions should pay special attention to any foreign subcontractors, as information security and data privacy standards may be different in other jurisdictions. Additionally, agreements should include the service provider's process for assessing the subcontractor's financial condition to fulfill contractual obligations.

D. Incentive Compensation Review

Financial institutions should also ensure that an effective process is in place to review and approve any incentive compensation that may be embedded in service provider contracts, including a review of whether existing governance and controls are adequate in light of risks arising from incentive compensation arrangements. As the service provider represents the institution by selling products or services on its behalf, the institution should consider whether the incentives provided might encourage the service provider to take imprudent risks. Inappropriately structured incentives may result in reputational damage, increased litigation, or other risks to the financial institution. An example of an inappropriate incentive would be one where variable fees or commissions encourage the service provider to direct customers to products with higher profit margins without due consideration of whether such products are suitable for the customer.

E. Oversight and Monitoring of Service Providers

To effectively monitor contractual requirements, financial institutions should establish acceptable performance metrics that the business line or relationship management determines to be indicative of acceptable performance levels. Financial institutions should ensure that

personnel with oversight and management responsibilities for service providers have the appropriate level of expertise and stature to manage the outsourcing arrangement. The oversight process, including the level and frequency of management reporting, should be risk-focused. Higher risk service providers may require more frequent assessment and monitoring and may require financial institutions to designate individuals or a group as a point of contact for those service providers. Financial institutions should tailor and implement risk mitigation plans for higher risk service providers that may include processes such as additional reporting by the service provider or heightened monitoring by the financial institution. Further, more frequent and stringent monitoring is necessary for service providers that exhibit performance, financial, compliance, or control concerns. For lower risk service providers, the level of monitoring can be lessened.

Financial condition: Financial institutions should have established procedures to monitor the financial condition of service providers to evaluate their ongoing viability. In performing these assessments, financial institutions should review the most recent financial statements and annual report with regard to outstanding commitments, capital strength, liquidity and operating results. If a service provider relies significantly on subcontractors to provide services to financial institutions, then the service provider's controls and due diligence regarding the subcontractors should also be reviewed.

***Internal controls*:** For significant service provider relationships, financial institutions should assess the adequacy of the provider's control environment. Assessments should include reviewing available audits or reports such as the American Institute of Certified Public Accountants' Service Organization Control 2 report.[10] If the service provider delivers information technology services, the financial institution can request the FFIEC Technology Service Provider examination report from its primary federal regulator. Security incidents at the service provider may also necessitate the institution to elevate its monitoring of the service provider.

Escalation of oversight activities: Financial institutions should ensure that risk management processes include triggers to escalate oversight and monitoring when service providers are failing to meet performance, compliance, control, or viability expectations. These procedures should include more frequent and stringent monitoring and follow-up on identified issues, on-site control reviews, and when an institution should exercise its right to audit a service provider's adherence to the terms of the agreement. Financial institutions should develop criteria for engaging alternative outsourcing arrangements and terminating the service provider contract in the event that identified issues are not adequately addressed in a timely manner.

F. Business Continuity and Contingency Considerations

Various events may affect a service provider's ability to provide contracted services. For example, services could be disrupted by a provider's performance failure, operational disruption, financial difficulty, or failure of business continuity and contingency plans during operational

[10] Refer to www.AICPA.org.

disruptions or natural disasters. Financial institution contingency plans should focus on critical services provided by service providers and consider alternative arrangements in the event that a service provider is unable to perform.[11] When preparing contingency plans, financial institutions should:

- Ensure that a disaster recovery and business continuity plan exists with regard to the contracted services and products;
- Assess the adequacy and effectiveness of a service provider's disaster recovery and business continuity plan and its alignment to their own plan;
- Document the roles and responsibilities for maintaining and testing the service provider's business continuity and contingency plans;
- Test the service provider's business continuity and contingency plans on a periodic basis to ensure adequacy and effectiveness; and
- Maintain an exit strategy, including a pool of comparable service providers, in the event that a contracted service provider is unable to perform.

G. Additional Risk Considerations

Suspicious Activity Report (SAR) reporting functions: The confidentiality of suspicious activity reporting makes the outsourcing of any SAR-related function more complex. Financial institutions need to identify and monitor the risks associated with using service providers to perform certain suspicious activity reporting functions in compliance with the Bank Secrecy Act (BSA). Financial institution management should ensure they understand the risks associated with such an arrangement and any BSA-specific guidance in this area.

***Foreign-based service providers*:** Financial institutions should ensure that foreign-based service providers are in compliance with applicable U.S. laws, regulations, and regulatory guidance. Financial institutions may also want to consider laws and regulations of the foreign-based provider's country or regulatory authority regarding the financial institution's ability to perform on-site review of the service provider's operations. In addition, financial institutions should consider the authority or ability of home country supervisors to gain access to the financial institution's customer information while examining the foreign-based service provider.

Internal audit: Financial institutions should refer to existing guidance on the engagement of independent public accounting firms and other outside professionals to perform work that has been traditionally carried out by internal auditors.[12] The Sarbanes-Oxley Act of

---

[11] For further guidance regarding business continuity planning with service providers, refer to the *FFIEC Business Continuity Booklet* (March 2008) at http://ithandbook.ffiec.gov/it-booklets/business-continuity-planning.aspx.

[12] Refer to SR 13-1, "Supplemental Policy Statement on the Internal Audit Function and Its Outsourcing," specifically the section titled, "Depository Institutions Subject to the Annual Audit and Reporting Requirements of Section 36 of the FDI Act" at http://www.federalreserve.gov/bankinforeg/srletters/sr1301.htm.
Refer also to SR 03-5, "Amended Interagency Guidance on the Internal Audit Function and its Outsourcing,"

2002 specifically prohibits a registered public accounting firm from performing certain non-audit services for a public company client for whom it performs financial statement audits.

Risk management activities: Financial institutions may outsource various risk management activities, such as aspects of interest rate risk and model risk management. Financial institutions should require service providers to provide information that demonstrates developmental evidence explaining the product components, design, and intended use, to determine whether the products and/or services are appropriate for the institution's exposures and risks.[13] Financial institutions should also have standards and processes in place for ensuring that service providers offering model risk management services, such as validation, do so in a way that is consistent with existing model risk management guidance.

---

particularly the section titled, "Institutions Not Subject to Section 36 of the FDI Act that are Neither Public Companies nor Subsidiaries of Public Companies" at http://www.federalreserve.gov/boarddocs/srletters/2003/sr0305.htm.

[13] Refer to SR 11-7, "Guidance on Model Risk Management" which informs financial institutions of the importance and risk to the use of models and the supervisory expectations that financial institutions should adhere to. http://www.federalreserve.gov/bankinforeg/srletters/sr1107.htm

Office of the Comptroller of the Currency
U.S. Department of the Treasury

OCC BULLETIN 2013-29

Subject: Third-Party Relationships
Date: October 30, 2013

To: Chief Executive Officers and Chief Risk Officers of All National Banks and Federal Savings Associations, Technology Service Providers, Department and Division Heads, All Examining Personnel, and Other Interested Parties

Description: Risk Management Guidance

Summary

This bulletin provides guidance to national banks and federal savings associations (collectively, banks) for assessing and managing risks associated with third-party relationships. A third-party relationship is any business arrangement between a bank and another entity, by contract or otherwise.[1]

The Office of the Comptroller of the Currency (OCC) expects a bank to practice effective risk management regardless of whether the bank performs the activity internally or through a third party. A bank's use of third parties does not diminish the responsibility of its board of directors and senior management to ensure that the activity is performed in a safe and sound manner and in compliance with applicable laws.[2]

This bulletin rescinds OCC Bulletin 2001-47, "Third-Party Relationships: Risk Management Principles," and OCC Advisory Letter 2000-9, "Third-Party Risk." This bulletin supplements and should be used in conjunction with other OCC and interagency issuances on third-party relationships and risk management listed in appendix B. In connection with the issuance of this bulletin, the OCC is applying to federal savings associations (FSA) certain guidance applicable to national banks, as indicated in appendix B.

Highlights

- A bank should adopt risk management processes commensurate with the level of risk and complexity of its third-party relationships.
- A bank should ensure comprehensive risk management and oversight of third-party relationships involving critical activities.
- An effective risk management process throughout the life cycle of the relationship includes
    - plans that outline the bank's strategy, identify the inherent risks of the activity, and detail how the bank selects, assesses, and oversees the third party.
    - proper due diligence in selecting a third party.
    - written contracts that outline the rights and responsibilities of all parties.
    - ongoing monitoring of the third party's activities and performance.
    - contingency plans for terminating the relationship in an effective manner.
    - clear roles and responsibilities for overseeing and managing the relationship and risk management process.
    - Documentation and reporting that facilitates oversight, accountability, monitoring, and risk management.
    - Independent reviews that allow bank management to determine that the bank's process aligns with its strategy and effectively manages risks.

Note for Community Banks

This guidance applies to all banks with third-party relationships. A community bank should adopt risk management practices commensurate with the level of risk and complexity of its third-party relationships. A community bank's board and management should identify those third-party relationships that involve critical activities and ensure the bank has risk management practices in place to assess, monitor, and manage the risks.

Background

Banks continue to increase the number and complexity of relationships with both foreign and domestic third parties, such as

- outsourcing entire bank functions to third parties, such as tax, legal, audit, or information technology operations.
- outsourcing lines of business or products.
- relying on a single third party to perform multiple activities, often to such an extent that the third party becomes an integral component of the bank's operations.
- working with third parties that engage directly with customers.[3]
- contracting with third parties that subcontract activities to other foreign and domestic providers.
- contracting with third parties whose employees, facilities, and subcontractors may be geographically concentrated.
- working with a third party to address deficiencies in bank operations or compliance with laws or regulations.

The OCC is concerned that the quality of risk management over third-party relationships may not be keeping pace with the level of risk and complexity of these relationships. The OCC has identified instances in which bank management has

- failed to properly assess and understand the risks and direct and indirect costs involved in third-party relationships.
- failed to perform adequate due diligence and ongoing monitoring of third-party relationships.
- entered into contracts without assessing the adequacy of a third party's risk management practices.
- entered into contracts that incentivize a third party to take risks that are detrimental to the bank or its customers, in order to maximize the third party's revenues.
- engaged in informal third-party relationships without contracts in place.

These examples represent trends whose associated risks reinforce the need for banks to maintain effective risk management practices over third-party relationships.

Risk Management Life Cycle

The OCC expects a bank to have risk management processes that are commensurate with the level of risk and complexity of its third-party relationships and the bank's organizational structures. Therefore, the OCC expects more comprehensive and rigorous oversight and management of third-party relationships that involve ***critical activities***—significant bank functions (e.g., payments, clearing, settlements, custody) or significant shared services (e.g., information technology), or other activities that

- could cause a bank to face significant risk[4] if the third party fails to meet expectations.
- could have significant customer impacts.
- require significant investment in resources to implement the third-party relationship and manage the risk.
- could have a major impact on bank operations if the bank has to find an alternate third party or if the outsourced activity has to be brought in-house.

An effective third-party risk management process follows a continuous life cycle for all relationships and incorporates the following phases:

Planning: Developing a plan to manage the relationship is often the first step in the third-party risk management process. This step is helpful for many situations but is necessary when a bank is considering contracts with third parties that involve critical activities.

Due diligence and third-party selection: Conducting a review of a potential third party before signing a contract[5] helps ensure that the bank selects an appropriate third party and understands and controls the risks posed by the relationship, consistent with the bank's risk appetite.

Contract negotiation: Developing a contract that clearly defines expectations and responsibilities of the third party helps to ensure the contract's enforceability, limit the bank's liability, and mitigate disputes about performance.

Ongoing monitoring: Performing ongoing monitoring of the third-party relationship once the contract is in place is essential to the bank's ability to manage risk of the third-party relationship.

Termination: Developing a contingency plan to ensure that the bank can transition the activities to another third party, bring the activities in-house, or discontinue the activities when a contract expires, the terms of the contract have been satisfied, in response to contract default, or in response to changes to the bank's or third party's business strategy.

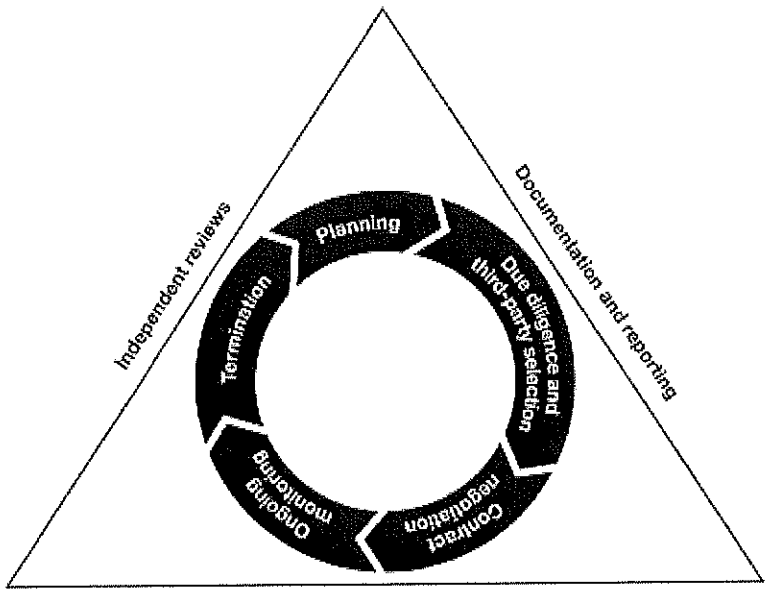
In addition, a bank should perform the following throughout the life cycle of the relationship as part of its risk management process:

Oversight and accountability: Assigning clear roles and responsibilities for managing third-party relationships and integrating the bank's third-party risk management process with its enterprise risk management framework enables continuous oversight and accountability.

Documentation and reporting: Proper documentation and reporting facilitates oversight, accountability, monitoring, and risk management associated with third-party relationships.

Independent reviews: Conducting periodic independent reviews of the risk management process enables management to assess whether the process aligns with the bank's strategy and effectively manages risk posed by third-party relationships.

Figure 1: Risk Management Life Cycle



Source: OCC

Planning

Before entering into a third-party relationship, senior management should develop a plan to manage the relationship. The management plan should be commensurate with the level of risk and complexity of the third-party relationship and should

- discuss the risks inherent in the activity.
- outline the strategic purposes (e.g., reduce costs, leverage specialized expertise or technology, augment resources, expand or enhance operations), legal and compliance aspects, and inherent risks associated with using third parties, and discuss how the arrangement aligns with the bank's overall strategic goals, objectives, and risk appetite.
- assess the complexity of the arrangement, such as the volume of activity, potential for subcontractors, the technology needed, and the likely degree of foreign-based third-party support.
- determine whether the potential financial benefits outweigh the estimated costs to control the risks (including estimated direct contractual costs and indirect costs to augment or alter bank processes, systems, or staffing to properly manage the third-party relationship or adjust or terminate existing contracts).
- consider how the third-party relationship could affect other strategic bank initiatives, such as large technology projects, organizational changes, mergers, acquisitions, or divestitures.
- consider how the third-party relationship could affect bank and dual employees[6] and what transition steps are needed to manage the impacts when the activities currently conducted internally are outsourced.
- assess the nature of customer interaction with the third party and potential impact the relationship will have on the bank's customers—including access to or use of those customers' confidential information, joint marketing or franchising arrangements, and handling of customer complaints—and outline plans to manage these impacts.
- assess potential information security implications including access to the bank's systems and to its confidential information.
- consider the bank's contingency plans in the event the bank needs to transition the activity to another third party or bring it in-house.
- assess the extent to which the activities are subject to specific laws and regulations (e.g., privacy, information security, Bank Secrecy Act/Anti-Money Laundering (BSA/AML), fiduciary requirements).
- consider whether the selection of the third party is consistent with the bank's broader corporate policies and practices including its diversity policies and practices.
- detail how the bank will select, assess, and oversee the third party, including monitoring the third party's compliance with the contract.
- be presented to and approved by the bank's board of directors when critical activities are involved.

Due Diligence and Third-Party Selection

A bank should conduct due diligence on all potential third parties before selecting and entering into contracts or relationships. A bank should not rely solely on experience with or prior knowledge of the third party as a proxy for an objective, in-depth assessment of the third party's ability to perform the activity in compliance with all applicable laws and regulations and in a safe and sound manner.

The degree of due diligence should be commensurate with the level of risk and complexity of the third-party relationship. More extensive due diligence is necessary when a third-party relationship involves critical activities. On-site visits may be useful to understand fully the third party's operations and capacity. If the bank uncovers information that warrants additional scrutiny, it should broaden the scope or assessment methods of the due diligence as needed.

The bank should consider the following during due diligence:

Strategies and Goals

Review the third party's overall business strategy and goals to ensure they do not conflict with those of the bank. Consider how the third party's current and proposed strategic business

arrangements (such as mergers, acquisitions, divestitures, joint ventures, or joint marketing initiatives) may affect the activity. Also consider reviewing the third party's service philosophies, quality initiatives, efficiency improvements, and employment policies and practices.

Legal and Regulatory Compliance

Evaluate the third party's legal and regulatory compliance program to determine whether the third party has the necessary licenses to operate and the expertise, processes, and controls to enable the bank to remain compliant with domestic and international laws and regulations. Check compliance status with regulators and self-regulatory organizations as appropriate.

Financial Condition

Assess the third party's financial condition, including reviews of the third party's audited financial statements. Evaluate growth, earnings, pending litigation, unfunded liabilities, and other factors that may affect the third party's overall financial stability. Depending on the significance of the third-party relationship, the bank's analysis may be as comprehensive as if extending credit to the third party.

Business Experience and Reputation

Evaluate the third party's depth of resources and previous experience providing the specific activity. Assess the third party's reputation, including history of customer complaints or litigation. Determine how long the third party has been in business, its market share for the activities, and whether there have been significant changes in the activities offered or in its business model. Conduct reference checks with external organizations and agencies such as the industry associations, Better Business Bureau, Federal Trade Commission, state attorneys general offices, state consumer affairs offices, and similar foreign authorities. Check U.S. Securities and Exchange Commission or other regulatory filings. Review the third party's Web sites and other marketing materials to ensure that statements and assertions are in-line with the bank's expectations and do not overstate or misrepresent activities and capabilities. Determine whether and how the third party plans to use the bank's name and reputation in marketing efforts.

Fee Structure and Incentives

Evaluate the third party's normal fee structure and incentives for similar business arrangements to determine if the fee structure and incentives would create burdensome upfront fees or result in inappropriate risk taking by the third party or the bank.

Qualifications, Backgrounds, and Reputations of Company Principals

Ensure the third party periodically conducts thorough background checks on its senior management and employees as well as on subcontractors who may have access to critical systems or confidential information. Ensure that third parties have policies and procedures in place for removing employees who do not meet minimum background check requirements.

Risk Management

Evaluate the effectiveness of the third party's risk management program, including policies, processes, and internal controls. Where applicable, determine whether the third party's internal audit function independently and effectively tests and reports on the third party's internal controls. Evaluate processes for escalating, remediating, and holding management accountable for concerns identified during audits or other independent tests. If available, review Service Organization Control (SOC) reports, prepared in accordance with the American Institute of Certified Public Accountants Statement on Standards for Attestation Engagements No. 16 (SSAE 16). Consider whether these reports contain sufficient information to assess the third party's risk or whether additional scrutiny is required through an audit by the bank or other third party at the bank's request. Consider any certification by independent third parties for compliance with domestic or international internal control standards (e.g., the National Institute of Standards and Technology and the International Standards Organization).

Information Security

Assess the third party's information security program. Determine whether the third party has sufficient experience in identifying, assessing, and mitigating known and emerging threats and vulnerabilities. When technology is necessary to support service delivery, assess the third party's infrastructure and application security programs, including the software development life cycle and results of vulnerability and penetration tests. Evaluate the third party's ability to implement effective and sustainable corrective actions to address deficiencies discovered during testing.

Management of Information Systems

Gain a clear understanding of the third party's business processes and technology that will be used to support the activity. When technology is a major component of the third-party relationship, review both the bank's and the third party's information systems to identify gaps in service-level expectations, technology, business process and management, or interoperability issues. Review the third party's processes for maintaining accurate inventories of its technology and its subcontractors. Assess the third party's change management processes to ensure that clear roles, responsibilities, and segregation of duties are in place. Understand the third party's performance metrics for its information systems and ensure they meet the bank's expectations.

Resilience

Assess the third party's ability to respond to service disruptions or degradations resulting from natural disasters, human error, or intentional physical or cyber attacks. Determine whether the third party maintains disaster recovery and business continuity plans that specify the time frame to resume activities and recover data. Review the third party's telecommunications redundancy and resilience plans and preparations for known and emerging threats and vulnerabilities, such as wide-scale natural disasters, distributed denial of service attacks, or other intentional or unintentional events. Review the results of business continuity testing and performance during actual disruptions.

Incident-Reporting and Management Programs

Review the third party's incident reporting and management programs to ensure there are clearly documented processes and accountability for identifying, reporting, investigating, and escalating incidents. Ensure that the third party's escalation and notification processes meet the bank's expectations and regulatory requirements.

Physical Security

Evaluate whether the third party has sufficient physical and environmental controls to ensure the safety and security of its facilities, technology systems, and employees.

Human Resource Management

Review the third party's program to train and hold employees accountable for compliance with policies and procedures. Review the third party's succession and redundancy planning for key management and support personnel. Review training programs to ensure that the third party's staff is knowledgeable about changes in laws, regulations, technology, risk, and other factors that may affect the quality of the activities provided.

Reliance on Subcontractors

Evaluate the volume and types of subcontracted activities and the subcontractors' geographic locations. Evaluate the third party's ability to assess, monitor, and mitigate risks from its use of subcontractors and to ensure that the same level of quality and controls exists no matter where the subcontractors' operations reside. Evaluate whether additional concentration-related risks may arise from the third party's reliance on subcontractors and, if necessary, conduct similar due diligence on the third party's critical subcontractors.

Insurance Coverage

Verify that the third party has fidelity bond coverage to insure against losses attributable to dishonest acts, liability coverage for losses attributable to negligent acts, and hazard insurance covering fire, loss of data, and protection of documents. Determine whether the third party has insurance coverage for its intellectual property rights, as such coverage may not be available under a general commercial policy. The amounts of such coverage should be commensurate with the level of risk involved with the third party's operations and the type of activities to be provided.

Conflicting Contractual Arrangements With Other Parties

Obtain information regarding legally binding arrangements with subcontractors or other parties in cases where the third party has indemnified itself, as such arrangements may transfer risks to the bank. Evaluate the potential legal and financial implications to the bank of these contracts between the third party and its subcontractors or other parties.

Senior management should review the results of the due diligence to determine whether the third party is able to meet the bank's expectations and whether the bank should proceed with the third-party relationship. If the results do not meet expectations, management should recommend that the third party make appropriate changes, find an alternate third party, conduct the activity in-house, or discontinue the activity. As part of any recommended changes, the bank may need to supplement the third party's resources or increase or implement new controls to manage the risks. Management should present results of due diligence to the board when making recommendations for third-party relationships that involve critical activities.

Contract Negotiation

Once the bank selects a third party, management should negotiate a contract that clearly specifies the rights and responsibilities of each party to the contract. Additionally, senior management should obtain board approval of the contract before its execution when a third-party relationship will involve critical activities. A bank should review existing contracts periodically, particularly those involving critical activities, to ensure they continue to address pertinent risk controls and legal protections. Where problems are identified, the bank should seek to renegotiate at the earliest opportunity.

Contracts should generally address the following:

Nature and Scope of Arrangement

Ensure that the contract specifies the nature and scope of the arrangement. For example, a third-party contract should specifically identify the frequency, content, and format of the service, product, or function provided. Include in the contract, as applicable, such ancillary services as software or other technology support and maintenance, employee training, and customer service. Specify which activities the third party is to conduct, whether on or off the bank's premises, and describe the terms governing the use of the bank's information, facilities, personnel, systems, and equipment, as well as access to and use of the bank's or customers' information. When dual employees will be used, clearly articulate their responsibilities and reporting lines.[7]

Performance Measures or Benchmarks

Specify performance measures that define the expectations and responsibilities for both parties including conformance with regulatory standards or rules. Such measures can be used to motivate the third party's performance, penalize poor performance, or reward outstanding performance. Performance measures should not incentivize undesirable performance, such as encouraging processing volume or speed without regard for accuracy, compliance requirements, or adverse effects on customers. Industry standards for service-level agreements may provide a reference point for standardized services, such as payroll processing. For more customized activities, there may be no standard measures. Instead, the bank and third party should agree on appropriate measures.

Responsibilities for Providing, Receiving, and Retaining Information

Ensure that the contract requires the third party to provide and retain timely, accurate, and comprehensive information such as records and reports that allow bank management to monitor performance, service levels, and risks. Stipulate the frequency and type of reports required, for example: performance reports, control audits, financial statements, security reports, BSA/AML and Office of Foreign Asset Control (OFAC) compliance responsibilities and reports for monitoring potential suspicious activity, reports for monitoring customer complaint activity, and business resumption testing reports.

Ensure that the contract sufficiently addresses

- the responsibilities and methods to address failures to adhere to the agreement including the ability of both parties to the agreement to exit the relationship.
- the prompt notification of financial difficulty, catastrophic events, and significant incidents such as information breaches, data loss, service or system interruptions, compliance lapses, enforcement actions, or other regulatory actions.
- the bank's materiality thresholds and procedures for notifying the bank in writing whenever service disruptions, security breaches, or other events pose a significant risk to the bank.
- notification to the bank before making significant changes to the contracted activities, including acquisition, subcontracting, off-shoring, management or key personnel changes, or implementing new or revised policies, processes, and information technology.
- notification to the bank of significant strategic business changes, such as mergers, acquisitions, joint ventures, divestitures, or other business activities that could affect the activities involved.
- the ability of the third party to resell, assign, or permit access to the bank's data and systems to other entities.
- the bank's obligations to notify the third party if the bank implements strategic or operational changes or experiences significant incidents that may affect the third party.

The Right to Audit and Require Remediation

Ensure that the contract establishes the bank's right to audit, monitor performance, and require remediation when issues are identified. Generally, a third-party contract should include provisions for periodic independent internal or external audits of the third party, and relevant subcontractors, at intervals and scopes consistent with the bank's in-house functions to monitor performance with the contract. A bank should include in the contract the types and frequency of audit reports the bank is entitled to receive from the third party (e.g., financial, SSAE 16, SOC 1, SOC 2, and SOC 3 reports, and security reviews). Consider whether to accept audits conducted by the third party's internal or external auditors. Reserve the bank's right to conduct its own audits of the third party's activities or to engage an independent party to perform such audits. Audit reports should include a review of the third party's risk management and internal control environment as it relates to the activities involved and of the third party's information security program and disaster recovery and business continuity plans.

Responsibility for Compliance With Applicable Laws and Regulations

Ensure the contract addresses compliance with the specific laws, regulations, guidance, and self-regulatory standards applicable to the activities involved, including provisions that outline compliance with certain provisions of the Gramm-Leach-Bliley Act (GLBA) (including privacy and safeguarding of customer information); BSA/AML; OFAC; and Fair Lending and other consumer protection laws and regulations. Ensure that the contract requires the third party to maintain policies and procedures which address the bank's right to conduct periodic reviews so as to verify the third party's compliance with the bank's policies and expectations. Ensure that the contract states the bank has the right to monitor on an ongoing basis the third party's compliance with applicable laws, regulations, and policies and requires remediation if issues arise.

Cost and Compensation

Fully describe compensation, fees, and calculations for base services, as well as any fees based on volume of activity and for special requests. Ensure the contracts do not include burdensome upfront fees or incentives that could result in inappropriate risk taking by the bank or third party. Indicate which party is responsible for payment of legal, audit, and examination fees associated with the activities involved. Consider outlining cost and responsibility for purchasing and maintaining hardware and software. Specify the conditions under which the cost structure may be changed, including limits on any cost increases.

Ownership and License

State whether and how the third party has the right to use the bank's information, technology, and intellectual property, such as the bank's name, logo, trademark, and copyrighted material. Indicate whether any records generated by the third party become the bank's property. Include appropriate warranties on the part of the third party related to its acquisition of licenses for use of any intellectual property developed by other third parties. If the bank purchases software, establish escrow agreements to provide for the bank's access to source code and programs under certain conditions (e.g., insolvency of the third party).

Confidentiality and Integrity

Prohibit the third party and its subcontractors from using or disclosing the bank's information, except as necessary to provide the contracted activities or comply with legal requirements. If the third party receives bank customers' personally identifiable information, the contract should ensure that the third party implements and maintains appropriate security measures to comply with privacy regulations and regulatory guidelines. Specify when and how the third party will disclose, in a timely manner, information security breaches that have resulted in unauthorized intrusions or access that may materially affect the bank or its customers. Stipulate that intrusion notifications include estimates of the effects on the bank and specify corrective action to be taken by the third party. Address the powers of each party to change security and risk management procedures and requirements, and resolve any confidentiality and integrity issues arising out of shared use of facilities owned by the third party. Stipulate whether and how often the bank and the third party will jointly practice incident management plans involving unauthorized intrusions or other breaches in confidentiality and integrity.

Business Resumption and Contingency Plans

Ensure the contract provides for continuation of the business function in the event of problems affecting the third party's operations, including degradations or interruptions resulting from natural disasters, human error, or intentional attacks. Stipulate the third party's responsibility for backing up and otherwise protecting programs, data, and equipment, and for maintaining current and sound business resumption and contingency plans. Include provisions—in the event of the third party's bankruptcy, business failure, or business interruption—for transferring the bank's accounts or activities to another third party without penalty.

Ensure that the contract requires the third party to provide the bank with operating procedures to be carried out in the event business resumption and disaster recovery plans are implemented. Include specific time frames for business resumption and recovery that meet the bank's requirements, and when appropriate, regulatory requirements. Stipulate whether and how often the bank and the third party will jointly practice business resumption and disaster recovery plans.

Indemnification

Consider including indemnification clauses that specify the extent to which the bank will be held liable for claims that cite failure of the third party to perform, including failure of the third party to obtain any necessary intellectual property licenses. Carefully assess indemnification clauses that require the bank to hold the third party harmless from liability.

Insurance

Stipulate that the third party is required to maintain adequate insurance, notify the bank of material changes to coverage, and provide evidence of coverage where appropriate. Types of insurance coverage may include fidelity bond coverage, liability coverage, hazard insurance, and intellectual property insurance.

Dispute Resolution

Consider whether the contract should establish a dispute resolution process (arbitration, mediation, or other means) to resolve problems between the bank and the third party in an expeditious manner, and whether the third party should continue to provide activities to the bank during the dispute resolution period.

Limits on Liability

Determine whether the contract limits the third party's liability and whether the proposed limit is in proportion to the amount of loss the bank might experience because of the third party's failure to perform or to comply with applicable laws. Consider whether a contract would subject the bank to undue risk of litigation, particularly if the third party violates or is accused of violating intellectual property rights.

Default and Termination

Ensure that the contract stipulates what constitutes default, identifies remedies and allows opportunities to cure defaults, and stipulates the circumstances and responsibilities for termination. Determine whether it includes a provision that enables the bank to terminate the contract, upon reasonable notice and without penalty, in the event that the OCC formally directs the bank to terminate the relationship. Ensure the contract permits the bank to terminate the relationship in a timely manner without prohibitive expense. Include termination and notification requirements with time frames to allow for the orderly conversion to another third party. Provide for the timely return or destruction of the bank's data and other resources and ensure the contract provides for ongoing monitoring of the third party after the contract terms are satisfied as necessary. Clearly assign all costs and obligations associated with transition and termination.

Customer Complaints

Specify whether the bank or third party is responsible for responding to customer complaints. If it is the third party's responsibility, specify provisions that ensure that the third party receives and responds timely to customer complaints and forwards a copy of each complaint and response to the bank. The third party should submit sufficient, timely, and usable information to enable the bank to analyze customer complaint activity and trends for risk management purposes.

Subcontracting

Stipulate when and how the third party should notify the bank of its intent to use a subcontractor. Specify the activities that cannot be subcontracted or whether the bank prohibits the third party from subcontracting activities to certain locations or specific subcontractors. Detail the contractual obligations—such as reporting on the subcontractor's conformance with performance measures, periodic audit results, compliance with laws and regulations, and other contractual obligations. State the third party's liability for activities or actions by its subcontractors and which party is responsible for the costs and resources required for any additional monitoring and management of the subcontractors. Reserve the right to terminate the contract without penalty if the third party's subcontracting arrangements do not comply with the terms of the contract.

Foreign-Based Third Parties

Include in contracts with foreign-based third parties choice-of-law covenants and jurisdictional covenants that provide for adjudication of all disputes between the parties under the laws of a single, specific jurisdiction. Understand that such contracts and covenants may be subject, however, to the interpretation of foreign courts relying on local laws. Foreign courts and laws may differ substantially from U.S. courts and laws in the application and enforcement of choice-of-law

covenants, requirements on banks, protection of privacy of customer information, and the types of information that the third party or foreign governmental entities will provide upon request. Therefore, seek legal advice to ensure the enforceability of all aspects of a proposed contract with a foreign-based third party and other legal ramifications of each such arrangement.

OCC Supervision

In contracts with service providers, stipulate that the performance of activities by external parties for the bank is subject to OCC examination oversight, including access to all work papers, drafts, and other materials. The OCC treats as subject to 12 USC 1867(c) and 12 USC 1464(d)(7), situations in which a bank arranges, by contract or otherwise, for the performance of any applicable functions of its operations. Therefore, the OCC generally has the authority to examine and to regulate the functions or operations performed or provided by third parties to the same extent as if they were performed by the bank itself on its own premises.[8]

Ongoing Monitoring

Ongoing monitoring for the duration of the third-party relationship is an essential component of the bank's risk management process. More comprehensive monitoring is necessary when the third-party relationship involves critical activities. Senior management should periodically assess existing third-party relationships to determine whether the nature of the activity performed now constitutes a critical activity.

After entering into a contract with a third party, bank management should dedicate sufficient staff with the necessary expertise, authority, and accountability to oversee and monitor the third party commensurate with the level of risk and complexity of the relationship. Regular on site visits may be useful to understand fully the third party's operations and ongoing ability to meet contract requirements. Management should ensure that bank employees that directly manage third-party relationships monitor the third party's activities and performance. A bank should pay particular attention to the quality and sustainability of the third party's controls, and its ability to meet service-level agreements, performance metrics and other contractual terms, and to comply with legal and regulatory requirements.

The OCC expects the bank's ongoing monitoring of third-party relationships to cover the due diligence activities discussed earlier. Because both the level and types of risks may change over the lifetime of third-party relationships, a bank should ensure that its ongoing monitoring adapts accordingly. This monitoring may result in changes to the frequency and types of required reports from the third party, including service-level agreement performance reports, audit reports, and control testing results. In addition to ongoing review of third-party reports, some key areas of consideration for ongoing monitoring may include assessing changes to the third party's

- business strategy (including acquisitions, divestitures, joint ventures) and reputation (including litigation) that may pose conflicting interests and impact its ability to meet contractual obligations and service-level agreements.
- compliance with legal and regulatory requirements.
- financial condition.
- insurance coverage.
- key personnel and ability to retain essential knowledge in support of the activities.
- ability to effectively manage risk by identifying and addressing issues before they are cited in audit reports.
- process for adjusting policies, procedures, and controls in response to changing threats and new vulnerabilities and material breaches or other serious incidents.
- information technology used or the management of information systems.
- ability to respond to and recover from service disruptions or degradations and meet business resilience expectations.
- reliance on, exposure to, or performance of subcontractors; location of subcontractors; and the ongoing monitoring and control testing of subcontractors.
- agreements with other entities that may pose a conflict of interest or introduce reputation, operational, or other risks to the bank.

- ability to maintain the confidentiality and integrity of the bank's information and systems.
- volume, nature, and trends of consumer complaints, in particular those that indicate compliance or risk management problems.
- ability to appropriately remediate customer complaints.

Bank employees who directly manage third-party relationships should escalate to senior management significant issues or concerns arising from ongoing monitoring, such as an increase in risk, material weaknesses and repeat audit findings, deterioration in financial condition, security breaches, data loss, service or system interruptions, or compliance lapses. Additionally, management should ensure that the bank's controls to manage risks from third-party relationships are tested regularly, particularly where critical activities are involved. Based on the results of the ongoing monitoring and internal control testing, management should respond to issues when identified including escalating significant issues to the board.

Termination

A bank may terminate third-party relationships for various reasons, including

- expiration or satisfaction of the contract.
- desire to seek an alternate third party.
- desire to bring the activity in-house or discontinue the activity.
- breach of contract.

Management should ensure that relationships terminate in an efficient manner, whether the activities are transitioned to another third party or in-house, or discontinued. In the event of contract default or termination, the bank should have a plan to bring the service in-house if there are no alternate third parties. This plan should cover

- capabilities, resources, and the time frame required to transition the activity while still managing legal, regulatory, customer, and other impacts that might arise.
- risks associated with data retention and destruction, information system connections and access control issues, or other control concerns that require additional risk management and monitoring during and after the end of the third-party relationship.
- handling of joint intellectual property developed during the course of the arrangement.
- reputation risks to the bank if the termination happens as a result of the third party's inability to meet expectations.

The extent and flexibility of termination rights may vary with the type of activity.

Oversight and Accountability

The bank's board of directors (or a board committee) and senior management are responsible for overseeing the bank's overall risk management processes. The board, senior management, and employees within the lines of businesses who manage the third-party relationships have distinct but interrelated responsibilities to ensure that the relationships and activities are managed effectively and commensurate with their level of risk and complexity, particularly for relationships that involve critical activities:[9]

Board of Directors

- Ensure an effective process is in place to manage risks related to third-party relationships in a manner consistent with the bank's strategic goals, organizational objectives, and risk appetite.
- Approve the bank's risk-based policies that govern the third-party risk management process and identify critical activities.
- Review and approve management plans for using third parties that involve critical activities.
- Review summary of due diligence results and management's recommendations to use third parties that involve critical activities.
- Approve contracts with third parties that involve critical activities.

- Review the results of management's ongoing monitoring of third-party relationships involving critical activities.
- Ensure management takes appropriate actions to remedy significant deterioration in performance or address changing risks or material issues identified through ongoing monitoring.
- Review results of periodic independent reviews of the bank's third-party risk management process.

Senior Bank Management

- Develop and implement the bank's third-party risk management process.
- Establish the bank's risk-based policies to govern the third-party risk management process.
- Develop plans for engaging third parties, identify those that involve critical activities, and present plans to the board when critical activities are involved.
- Ensure appropriate due diligence is conducted on potential third parties and present results to the board when making recommendations to use third parties that involve critical activities.
- Review and approve contracts with third parties. Board approval should be obtained for contracts that involve critical activities.
- Ensure ongoing monitoring of third parties, respond to issues when identified, and escalate significant issues to the board.
- Ensure appropriate documentation and reporting throughout the life cycle for all third-party relationships.
- Ensure periodic independent reviews of third-party relationships that involve critical activities and of the bank's third-party risk management process. Analyze the results, take appropriate actions, and report results to the board.
- Hold accountable the bank employees within business lines or functions who manage direct relationships with third parties.
- Terminate arrangements with third parties that do not meet expectations or no longer align with the bank's strategic goals, objectives, or risk appetite.
- Oversee enterprise-wide risk management and reporting of third-party relationships.

Bank Employees Who Directly Manage Third-Party Relationships

- Conduct due diligence of third parties and report results to senior management.
- Ensure that third parties comply with the bank's policies and reporting requirements.
- Perform ongoing monitoring of third parties and ensure compliance with contract terms and service-level agreements.
- Ensure the bank or the third party addresses any issues identified.
- Escalate significant issues to senior management.
- Notify the third party of significant operational issues at the bank that may affect the third party.
- Ensure that the bank has regularly tested controls in place to manage risks associated with third-party relationships.
- Ensure that third parties regularly test and implement agreed-upon remediation when issues arise.
- Maintain appropriate documentation throughout the life cycle.
- Respond to material weaknesses identified by independent reviews.
- Recommend termination of arrangements with third parties that do not meet expectations or no longer align with the bank's strategic goals, objectives, or risk appetite.

Documentation and Reporting

A bank should properly document and report on its third-party risk management process and specific arrangements throughout their life cycle. Proper documentation and reporting facilitates the accountability, monitoring, and risk management associated with third parties and typically includes

- a current inventory of all third-party relationships, which should clearly identify those relationships that involve critical activities and delineate the risks posed by those relationships across the bank.[10]
- approved plans for the use of third-party relationships.
- due diligence results, findings, and recommendations.

- analysis of costs associated with each activity or third-party relationship, including any indirect costs assumed by the bank.
- executed contracts.
- regular risk management and performance reports required and received from the third party (e.g., audit reports, security reviews, and reports indicating compliance with service-level agreements).
- regular reports to the board and senior management on the results of internal control testing and ongoing monitoring of third parties involved in critical activities.
- regular reports to the board and senior management on the results of independent reviews of the bank's overall risk management process.

Independent Reviews

Senior management should ensure that periodic independent reviews are conducted on the third-party risk management process, particularly when a bank involves third parties in critical activities. The bank's internal auditor or an independent third party may perform the reviews, and senior management should ensure the results are reported to the board. Reviews may include assessing the adequacy of the bank's process for

- ensuring third-party relationships align with the bank's business strategy.
- identifying, assessing, managing, and reporting on risks of third-party relationships.
- responding to material breaches, service disruptions, or other material issues.
- identifying and managing risks associated with complex third-party relationships, including foreign-based third parties and subcontractors.
- involving multiple disciplines across the bank as appropriate during each phase of the third-party risk management life cycle.[11]
- ensuring appropriate staffing and expertise to perform due diligence and ongoing monitoring and management of third parties.
- ensuring oversight and accountability for managing third-party relationships (e.g., whether roles and responsibilities are clearly defined and assigned and whether the individuals possess the requisite expertise, resources, and authority).
- ensuring that conflicts of interest or appearances of conflicts of interest do not exist when selecting or overseeing third parties.
- identifying and managing concentration risks that may arise from relying on a single third party for multiple activities, or from geographic concentration of business due to either direct contracting or subcontracting agreements to the same locations.

Senior management should analyze the results of independent reviews to determine whether and how to adjust the bank's third-party risk management process, including policy, reporting, resources, expertise, and controls. Additionally, the results may assist senior management's understanding of the effectiveness of the bank's third-party risk management process so that they can make informed decisions about commencing new or continuing existing third-party relationships, bringing activities in-house, or discontinuing activities. Management should respond promptly and thoroughly to significant issues or concerns identified and escalate to the board if the risk posed is approaching the bank's risk appetite limits.

Supervisory Reviews of Third-Party Relationships

The OCC expects bank management to engage in a robust analytical process to identify, measure, monitor, and control the risks associated with third-party relationships and to avoid excessive risk taking that may threaten a bank's safety and soundness. A bank's failure to have an effective third-party risk management process that is commensurate with the level of risk, complexity of third-party relationships, and organizational structure of the bank may be *an unsafe and unsound banking practice.*

When reviewing third-party relationships, examiners should

- assess the bank's ability to oversee and manage its relationships.
- highlight and discuss material risks and any deficiencies in the bank's risk management process with the board of directors and senior management.

- carefully review the bank's plans for appropriate and sustainable remediation of such deficiencies, particularly those associated with the oversight of third parties that involve critical activities.
- follow existing guidance for citing deficiencies in supervisory findings and reports of examination, and recommend appropriate supervisory actions. These actions may range from citing the deficiencies in Matters Requiring Attention to recommending formal enforcement action.
- consider the findings when assigning the management component of the Federal Financial Institutions Examination Council's (FFIEC) Uniform Financial Institutions Rating System (CAMELS ratings).[12] Serious deficiencies may result in management being deemed less than satisfactory.
- reflect the associated risks in their overall assessment of the bank's risk profile.

When circumstances warrant, the OCC may use its authority to examine the functions or operations performed by a third party on the bank's behalf. Such examinations may evaluate safety and soundness risks, the financial and operational viability of the third party to fulfill its contractual obligations, compliance with applicable laws and regulations, including consumer protection, fair lending, BSA/AML and OFAC laws, and whether the third party engages in unfair or deceptive acts or practices in violation of federal or applicable state law. The OCC will pursue appropriate corrective measures, including enforcement actions, to address violations of law and regulations or unsafe or unsound banking practices by the bank or its third party. The OCC has the authority to assess a bank a special examination or investigation fee when the OCC examines or investigates the activities of a third party for the bank.

Further Information

"For further information, contact John Eckert, Director, Operational Risk and Core Policy at (202) 649-7163 or john.eckert@occ.treas.gov [mailto:john.eckert@occ.treas.gov], or (202) 649-6550.

John C. Lyons Jr.
Senior Deputy Comptroller and Chief National Bank Examiner

Appendix A: Risks Associated With Third-Party Relationships
Appendix B: References

APPENDIX A: Risks Associated With Third-Party Relationships

Use of third parties reduces management's direct control of activities and may introduce new or increase existing risks, specifically, operational, compliance, reputation, strategic, and credit risks and the interrelationship of these risks. Increased risk most often arises from greater complexity, ineffective risk management by the bank, and inferior performance by the third party. Refer to the "Bank Supervision Process" booklet of the *Comptroller's Handbook* for an expanded discussion of banking risks and their definitions.

Operational Risk

Operational risk is present in all products, services, functions, delivery channels, and processes. Third-party relationships may increase a bank's exposure to operational risk because the bank may not have direct control of the activity performed by the third party.

Operational risk can increase significantly when third-party relationships result in concentrations. Concentrations may arise when a bank relies on a single third party for multiple activities, particularly when several of the activities are critical to bank operations. Additionally, geographic concentrations can

arise when a bank's own operations and that of its third parties and subcontractors are located in the same region or are dependent on the same critical power and telecommunications infrastructures.

Compliance Risk

Compliance risk exists when products, services, or systems associated with third-party relationships are not properly reviewed for compliance or when the third party's operations are not consistent with laws, regulations, ethical standards, or the bank's policies and procedures. Such risks also arise when a third party implements or manages a product or service in a manner that is unfair, deceptive, or abusive to the recipient of the product or service. Compliance risk may arise when a bank licenses or uses technology from a third party that violates a third party's intellectual property rights. Compliance risk may also arise when the third party does not adequately monitor and report transactions for suspicious activities to the bank under the BSA or OFAC. The potential for serious or frequent violations or noncompliance exists when a bank's oversight program does not include appropriate audit and control features, particularly when the third party is implementing new bank activities or expanding existing ones, when activities are further subcontracted, when activities are conducted in foreign countries, or when customer and employee data is transmitted to foreign countries.

Compliance risk increases when conflicts of interest between a bank and a third party are not appropriately managed, when transactions are not adequately monitored for compliance with all necessary laws and regulations, and when a bank or its third parties have not implemented appropriate controls to protect consumer privacy and customer and bank records. Compliance failures by the third party could result in litigation or loss of business to the bank and damage to the bank's reputation.

Reputation Risk

Third-party relationships that do not meet the expectations of the bank's customers expose the bank to reputation risk. Poor service, frequent or prolonged service disruptions, significant or repetitive security lapses, inappropriate sales recommendations, and violations of consumer law and other law can result in litigation, loss of business to the bank, or negative perceptions in the marketplace. Publicity about adverse events surrounding the third parties also may increase the bank's reputation risk. In addition, many of the products and services involved in franchising arrangements expose banks to higher reputation risks. Franchising the bank's attributes often includes direct or subtle reference to the bank's name. Thus, the bank is permitting its attributes to be used in connection with the products and services of a third party. In some cases, however, it is not until something goes wrong with the third party's products, services, or client relationships, that it becomes apparent to the third party's clients that the bank is involved or plays a role in the transactions. When a bank is offering products and services actually originated by third parties as its own, the bank can be exposed to substantial financial loss and damage to its reputation if it fails to maintain adequate quality control over those products and services and adequate oversight over the third party's activities.

Strategic Risk

A bank is exposed to strategic risk if it uses third parties to conduct banking functions or offer products and services that are not compatible with the bank's strategic goals, cannot be effectively monitored and managed by the bank, or do not provide an adequate return on investment. Strategic risk exists in a bank that uses third parties in an effort to remain competitive, increase earnings, or control expense without fully performing due diligence reviews or implementing the appropriate risk management infrastructure to oversee the activity. Strategic risk also arises if management does not possess adequate expertise and experience to oversee properly the third-party relationship.

Conversely, strategic risk can arise if a bank does not use third parties when it is prudent to do so. For example, a bank may introduce strategic risk when it does not leverage third parties that possess greater expertise than the bank does internally, when the third party can more cost effectively supplement internal expertise, or when the third party is more efficient at providing a service with better risk management than the bank can provide internally.

Credit Risk

Credit risk may arise when management has exercised ineffective due diligence and oversight of third parties that market or originate certain types of loans on the bank's behalf, resulting in low-quality receivables and loans. Ineffective oversight of third parties can also result in poor account management, customer service, or collection activities. Likewise, where third parties solicit and refer customers, conduct underwriting analysis, or set up product programs on behalf of the bank, substantial credit risk may be transferred to the bank if the third party is unwilling or unable to fulfill its obligations.

Credit risk also may arise from country or sovereign exposure. To the extent that a bank engages a foreign-based third party, either directly or through subcontractors, the bank may expose itself to country risk.

APPENDIX B: References

Additional guidance about third-party relationships and risk management practices can be found in the following documents.[13]

OCC Guidance

Issuance	Date	Subject	Description/Applicability to FSAs
Comptroller's Handbook	Various	Asset Management series	Each of the booklets in the Comptroller's Handbook Asset Management series provides guidance on oversight of third-party providers. **Applies to FSAs.**
Comptroller's Handbook	September 2013	Other Real Estate Owned	Provides guidance on managing foreclosed properties, including risk management of third-party relationships. **Applies to FSAs.**
Comptroller's Handbook	April 2012	SAFE Act	Provides procedures for examining mortgage loan originator (MLO) activities for compliance with the Secure & Fair Enforcement & Licensing Act of 2008, which mandates a nationwide licensing and registration system for residential MLOs. MLOs may be employees of a bank or third-party vendors. **Applies to FSAs.**
Comptroller's Handbook	May 2011	Servicemembers Civil Relief Act of 2003 (SCRA)	Provides guidance on SCRA requirements applicable to banks and servicers, as a large number of banks outsource loan-servicing functions such as credit administration to third-party servicers.
Comptroller's Handbook	December 2010	Truth in Lending Act	Provides guidance to banks and servicers on the content and timing of disclosures; interest rate calculations; and prohibited activities.
Comptroller's Handbook	September 2010	Real Estate Settlement Procedures	Provides guidance to banks and servicers on the content and timing of pre-settlement and settlement disclosures to borrowers and on prohibited practices.
Comptroller's Handbook	January 2010	Fair Lending	Provides guidance on indicators of potential disparate treatment in loan servicing and loss mitigation; use of vendor-designed credit scorecards; and guidance on evaluating third parties.
Comptroller's Handbook	April 2003	Internal and External Audits	Provides guidelines for banks that outsource internal audit.
Comptroller's Handbook	December 2001	Merchant Processing	Provides guidance on risk management of third-party processors.

Comptroller's Handbook	February 1994	Retail Nondeposit Investment Sales	Provides guidance on risk management and board oversight of third-party vendors selling nondeposit investment products. (See OCC Bulletin 1994-13)
Alert 2012-16	December 21, 2012	Information Security: Distributed Denial of Service Attacks and Customer Account Fraud	Highlights the risks related to these attacks; raises awareness for banks to be prepared to mitigate associated risks. Preparation may include ensuring sufficient resources in conjunction with pre-contracted third-party servicers that can assist in managing the internet-based traffic flow. **Applies to FSAs.**
Alert 2001-4	April 24, 2001	Network Securities Vulnerabilities	Alerts banks to review contracts with service providers to ensure that security maintenance and reporting responsibilities are clearly described.
News Release 2013-116	July 17, 2013	OCC Statement Regarding Oversight of Debt Collection and Debt Sales	Appendix provides guidance on the due diligence and ongoing monitoring of third parties to which banks sell consumer debt. **Applies to FSAs.**
News Release 2012-93	June 21, 2012	Regulators Issue Joint Guidance to Address Mortgage Servicer Practices that Affect Servicemembers	Provides guidance to banks and mortgage servicers, including ensuring that their employees are adequately trained about the options available for homeowners with permanent change of station orders. **Applies to FSAs.**
Bulletin 2013-10	March 29, 2013	Flood Disaster Protection Act: Interagency Statement on Effective Dates of Certain Provisions of the Biggert–Waters Act and Impact on Proposed Interagency Questions and Answers	Provides guidance to lenders or their servicers regarding the contents of notifications to borrowers about flood insurance renewals, force placement to ensure continuity of coverage, use of private flood insurance policies, related insurance fees, and escrow accounts. Provides summaries of new requirements for disclosure contents and timing. **Applies to FSAs.**
Bulletin 2011-39	September 22, 2011	Fair Credit Reporting and Equal Credit Opportunity Acts—Risk-Based Pricing Notices: Final Rules	Provides guidance on notification requirements (timing, content) when adverse credit decision relies on a credit score, including those generated by third-party vendors (i.e., consumer reporting agencies). **Applies to FSAs.**
Bulletin 2011-30	July 6, 2011	Counterparty Credit Risk Management: Interagency Supervisory Guidance	Addresses some of the weaknesses highlighted by the recent financial crisis and reinforces sound governance of counterparty credit risk (CCR) management practices through prudent board and senior management oversight and an effective CCR management framework. **Applies to FSAs with the issuance of this bulletin.**
Bulletin 2011-29	June 30, 2011	Foreclosure Management: Supervisory Guidance	Discusses third-party vendor management and reaffirms expectations that management should properly structure, carefully conduct, and prudently manage relationships with third-party vendors, including outside law firms assisting in the foreclosure process. **Applies to FSAs.**
Bulletin 2011-27	June 28, 2011	Prepaid Access Programs: Risk Management Guidance and Sound Practices	Highlights the risks and provides risk management guidance concerning prepaid access programs. **Applies to FSAs.**
Bulletin 2011-26	June 28, 2011	Authentication in an Internet Banking	Reinforces the guidance's risk management framework and updates expectations regarding

		Environment: Supplement	banks' authentications systems and practices whether they are provided internally or by a technology service provider. **Applies to FSAs.**
Bulletin 2011-12	April 4, 2011	Sound Practices for Model Risk Management: Supervisory Guidance	Includes guidance on the use of third-party models. **Applies to FSAs.**
Bulletin 2011-11	March 29, 2011	Risk Management Elements: Collective Investment Funds and Outsourcing Arrangements	Expands upon long-standing guidance on sound risk management and beneficiary/participant protections for bank-offered collective investment funds (CIF). The focus is on supervisory concerns that arise if a bank delegates responsibility for a bank CIF to a third-party service provider, such as a registered investment adviser. **Applies to FSAs with the issuance of this bulletin.**
Bulletin 2010-42	December 10, 2010	Sound Practices for Appraisals and Evaluations: Interagency Appraisal and Evaluation Guidelines	Provides guidance regarding a bank's responsibility for selecting appraisers and people performing evaluations based on their competence, experience, and knowledge of the market and type of property being valued. **Applies to FSAs.**
Bulletin 2010-30	August 16, 2010	Reverse Mortgages: Interagency Guidance	Provides guidance on managing the compliance and reputation risks when making, purchasing, or servicing reverse mortgages through a third party, such as a mortgage broker or correspondent. **Applies to FSAs.**
Bulletin 2010-7	February 18, 2010	Tax Refund Anticipation Loans: Guidance on Consumer Protection and Safety and Soundness	Provides guidance to enhance, clarify, and increase awareness regarding the measures the OCC expects to see in place for tax refund-related products offered by banks, including issues related to reliance on third-party tax return preparers who interact with consumers.
Bulletin 2010-1	January 8, 2010	Interest Rate Risk: Interagency Advisory on Interest Rate Risk Management	Includes guidance on selection, control frameworks, and validation of third-party asset liability management models. **Applies to FSAs.**
Bulletin 2009-15	May 22, 2009	Investment Securities: Risk Management and Lessons Learned	Provides guidance for banks that use the services of third parties who compile and provide investment analytics for bank management.
Bulletin 2008-12	April 24, 2008	Payment Processors: Risk Management Guidance	Provides guidance to banks regarding relationships with third-party processors and requirements for effective due diligence, underwriting, and monitoring. **Applies to FSAs with the issuance of this bulletin.**
Bulletin 2008-5	March 6, 2008	Conflicts of Interest: Risk Management Guidance—Divestiture of Certain Asset Management Businesses	Provides guidance for banks that contemplate divestiture of affiliated funds and associated advisers, whether directly, or through their broader corporate organizations.
Bulletin 2008-4	February 2, 2008	Flood Disaster Protection Act: Flood Hazard Determination Practices	Provides guidance to banks that outsource flood hazard determinations to third-party servicers to ensure that appropriate information is used when performing flood determinations and that revision dates be included in the determination form. **Applies to FSAs with the issuance of this bulletin.**
Bulletin 2006-47	December 13, 2006	Allowance for Loan and Lease Losses	Includes guidance for when some or the entire loan review function and the validation of the ALLL

		(ALLL): Guidance and Frequently Asked Questions (FAQs) on the ALLL	methodology is outsourced to a qualified external party, and identifies the minimum objectives of a loan review program. **Applies to FSAs.**
Bulletin 2006-39	September 1, 2006	Automated Clearing House Activities: Risk Management Guidance	Provides guidance for banks and examiners on managing the risks of automated clearing house (ACH) activity, which can include new and evolving types of ACH transactions as well as new participants in the ACH network, including certain merchants and third parties known as third-party senders. **Applies to FSAs with the issuance of this bulletin.**
Bulletin 2005-35	October 12, 2005	Authentication in an Internet Banking Environment: Interagency Guidance	Highlights requirements for banks to use this guidance when evaluating and implementing authentication systems and practices whether they are provided internally or by a technology service provider. **Applies to FSAs.**
Bulletin 2005-27	August 4, 2005	Real Estate Settlement Procedures Act (RESPA): Sham Controlled Business Arrangements	Provides guidance on determining if a RESPA settlement service provider (often a third-party servicer or vendor) is a "controlled business arrangement" and therefore entitled to certain exemptions. **Applies to FSAs with the issuance of this bulletin.**
Bulletin 2005-22	May 16, 2005	Home Equity Lending: Credit Risk Management Guidance	Sets forth regulatory expectations for enhanced risk management practices, including management of third-party originations. **Applies to FSAs.**
Bulletin 2005-13	April 14, 2005	Response Programs for Unauthorized Access to Customer Information and Customer Notice: Final Guidance: Interagency Guidance	Provides guidance on banks implementing a response program to address unauthorized access to customer information maintained by the institution or its service providers. **Applies to FSAs.**
Bulletin 2005-1	January 12, 2005	Proper Disposal of Consumer Information: Final Rule	Sets standards for information security. Requires agreements with service providers on disposal. Describes duties of users of consumer reports regarding identity theft. **Applies to FSAs with the issuance of this bulletin.**
Bulletin 2004-47	October 27, 2004	FFIEC Guidance: Risk Management for the Use of Free and Open Source Software (FOSS)	Provides guidance for institutions considering using or deploying FOSS regardless of whether it will be provided internally or by a third-party service provider. **Applies to FSAs.**
Bulletin 2004-20	May 10, 2004	Risk Management of New, Expanded, or Modified Bank Products and Services: Risk Management Process	Reminds banks of the risk management process they should follow to prudently manage the risks associated with new, expanded, or modified bank products and services, including those provided by third parties.
Bulletin 2003-15	April 23, 2003	Weblinking: Interagency Guidance on Weblinking Activity	Provides guidance to institutions that develop and maintain their own Web sites, as well as institutions that use third-party service providers for this function. **Applies to FSAs.**
Bulletin 2003-12	March 17, 2003	Interagency Policy Statement on Internal Audit and Internal Audit Outsourcing: Revised Guidance on	Reflects developments within the financial, audit, and regulatory industries, particularly the Sarbanes –Oxley Act of 2002 that established numerous independence parameters for audit firms that provide external audit, outsourced internal audit,

		Internal Audit and Its Outsourcing	and other non-audit services for financial institutions. **Applies to FSAs.**
Bulletin 2002-16	May 15, 2002	Bank Use of Foreign-Based Third-Party Service Providers: Risk Management Guidance	Provides guidance on managing the risks that may arise from outsourcing relationships with foreign-based third-party service providers, and addresses the need for banks to establish relationships with foreign-based third-party service providers in a way that does not diminish the ability of the OCC to timely access data or information needed for supervisory activities. **Applies to FSAs with the issuance of this bulletin.**
Bulletin 2002-03	January 15, 2002	Real Estate Settlement Procedures Act: Examiner Guidance—Mark-ups of Settlement Service Fees	Provides guidance on determining if a RESPA settlement service provider (often a third-party servicer or vendor) is charging more for a settlement service provided by a third party than is actually paid to the third party and the third party is not involved in the mark-up, which is prohibited by RESPA Section 8(b) (implemented by Regulation X) in most but not all states. **Applies to FSAs with the issuance of this bulletin.**
Bulletin 2001-51	December 12, 2001	Privacy of Consumer Financial Information: Small Bank Compliance Guide	Includes guidance for banks to evaluate agreements with nonaffiliated third parties that involve the disclosure of consumer information. **Applies to FSAs.**
Bulletin 2001-12	February 28, 2001	Bank-Provided Account Aggregation Services: Guidance to Banks	Includes guidance for banks that offer aggregation services through third-party service providers.
Bulletin 2001-8	February 15, 2001	Guidelines Establishing Standards for Safeguarding Customer Information: Final Guidelines	Alerts banks that oversight program of service providers should include confirmation that the providers have implemented appropriate measures designed to meet the objectives of the guidelines. **Applies to FSAs with the issuance of this bulletin.**
Bulletin 2000-25	September 8, 2000	Privacy Laws and Regulations: Summary of Requirements	Includes guidance for banks to evaluate agreements with third parties that involve the disclosure of consumer information. **Applies to FSAs with the issuance of this bulletin.**
Bulletin 2000-14	May 15, 2000	Infrastructure Threats—Intrusion Risks: Message to Bankers and Examiners	Provides guidance on how to prevent, detect, and respond to intrusions into bank computer systems, including outsourced systems.
Bulletin 1999-14	March 29, 1999	Real Estate Settlement Procedures Act: Statement of Policy—Lender Payments to Mortgage Brokers	Provides guidance on services normally performed in loan origination, including those often performed by a third-party servicer or vendor. **Applies to FSAs with the issuance of this bulletin.**
Bulletin 1998-3	March 17, 1998	Technology Risk Management: Guidance for Bankers and Examiners	Includes a short description of a bank's responsibility with regard to outsourcing its technology products and services. **Applies to FSAs with the issuance of this bulletin.**
Bulletin 1996-48	September 3, 1996	Stored Value Card Systems: Information for Bankers and Examiners	Provides basic information to assist banks in identifying and managing risks involved in stored value systems. **Applies to FSAs with the issuance of this bulletin.**
		Payroll Card Systems	

Advisory Letter 2004-6	May 6, 2004		Advises banks engaged in payroll cards systems involving nonbank third parties to fully comply with OCC guidance on third-party relationships.
Advisory Letter 2002-3	March 22, 2002	Guidance on Unfair or Deceptive Acts or Practices	Describes legal standards and provides guidance on unfair or deceptive acts and practices. Cross references other OCC guidance on: selecting a third-party vendor; monitoring vendor performance; maintaining proper documentation about vendor management; review of contractual arrangements; compensation concerns; monitoring consumer complaints; payment procedures; and loan collection activities.
Advisory Letter 2000-11	November 27, 2000	Title Loan Programs	Alerts banks to OCC concerns over title loan programs, including the involvement of third-party vendors.
Advisory Letter 2000-10	November 27, 2000	Payday Lending	Alerts banks to OCC concerns over payday lending programs, including the involvement of third-party vendors. **Applies to FSAs.**
Banking Circular 181	August 2, 1984	Purchases of Loans in Whole or in Part-Participations	Describes prudent purchases of loans from and loan participations with third parties. **Applies to FSAs with the issuance of this bulletin.**

FFIEC Handbooks

Issuance	**Date**	**Subject**	**Description**
FFIEC Bank Secrecy Act/ Anti-Money Laundering Examination Manual	April 29, 2010	Bank Secrecy Act and Anti-Money Laundering	Provides guidance on identifying and controlling risks associated with money laundering and terrorist financing, including third-party payment processors and professional service providers.
FFIEC Information Technology Examination Handbook	Various	"Outsourcing Technology Services" and "Supervision of Technology Service Providers"	Provides guidance on managing risks associated with the outsourcing of IT services. Several other booklets of the FFIEC IT Examination Handbook also provide guidance addressing third-party relationships.

---

[1] Third-party relationships include activities that involve outsourced products and services, use of independent consultants, networking arrangements, merchant payment processing services, services provided by affiliates and subsidiaries, joint ventures, and other business arrangements where the bank has an ongoing relationship or may have responsibility for the associated records. Affiliate relationships are also subject to sections 23A and 23B of the Federal Reserve Act (12 USC 371c and 12 USC 371c-1) as implemented in Regulation W (12 CFR 223). Third-party relationships generally do not include customer relationships.

[2] An OCC-supervised bank that provides services to another OCC-supervised bank is held to the same standards of due diligence, controls, and oversight as is a non-bank entity.

[3] For example, in franchising arrangements, the bank lends its name or regulated entity status to activities originated or predominantly conducted by others. Thus, the bank is permitting its attributes to be used in connection with the products and services of a third party. The risks to the bank from these franchising arrangements vary based on the terms of the agreement between the bank and the third party and the nature of the services offered. When a bank is offering products and services originated by third parties as its own, the bank can be exposed to substantial financial loss and damage to its reputation if it fails to maintain adequate quality control over those products and services and adequate oversight over the third-party activities. Risk may

also increase when the third party relies on the bank's regulated entity status and offers services or products through the bank with fees, interest rates, or other terms that cannot be offered by the third party directly.

[4] Refer to appendix A for a discussion of risks associated with third-party relationships.

[5] Except for nondisclosure agreements that may be required in order for the bank to conduct due diligence.

[6] Dual employees are employed by both the bank and the third party.

[7] If the bank enters into a written arrangement under which a broker registered under the securities laws offers brokerage services on or off the premises of the bank, the bank should ensure that the arrangement qualifies for the exception in the Securities and Exchange Act of 1934, 15 USC 78c(a)(4)(B)(i), and Regulation R, 12 CFR 218.700-701 and 17 CFR 247.700-701, for third-party brokerage arrangements. Otherwise, the bank may be required to register as a securities broker under the federal securities laws. The bank also should ensure compliance with regulatory requirements if bank employees receive fees for referrals to the third-party broker.

[8] Before conducting an examination of a third party that is a functionally regulated affiliate (FRA), the OCC is required to give notice to and consult with the FRA's primary regulator and, to the fullest extent possible, avoid duplication of examination activities, reporting requirements, and requests for information. See 12 USC 1831v.

[9] When a third-party relationship involves critical activities, a bank may need to consider appointing a senior officer to provide oversight of that relationship.

[10] Under 12 USC 1867(c)(2), national banks are required to notify the OCC of the existence of a servicing relationship. FSAs are subject to similar requirements set forth in 12 USC 1464(d)(7)(D)(ii) and 12 USC 1867(c)(2). The OCC implements this notification requirement by requiring banks to maintain a current inventory of all third-party relationships and make it available to examiners upon request.

[11] In addition to the functional business units, this may include information technology, identity and access management, physical security, information security, business continuity, compliance, legal, risk management, and human resources.

[12] The CAMELS rating is an overall assessment of a bank based on six individual ratings; the word CAMELS is an acronym for these individual elements of regulatory assessment (capital adequacy, asset quality, management, earnings, liquidity, and sensitivity to market risk).

[13] All guidance applies to national banks. Guidance not currently applicable to FSAs (as noted in this appendix) is undergoing review through the OCC's policy integration efforts.

AGENCY VRM GUIDANCE W/ FINTECH FOCUS

Examination Guidance for Third-Party Lending

As of July 29, 2016

Purpose

Third-party lending arrangements may provide institutions with the ability to supplement, enhance, or expedite lending services for their customers. Engaging in third-party lending arrangements may also enable institutions to lower costs of delivering credit products and to achieve strategic or profitability goals. However, these arrangements also present a number of risks that require effective management. This guidance provides information on third-party lending activities[1] and supplements the FDIC's Guidance for Managing Third-Party Risk ("Third-Party Guidance").

The Third-Party Guidance applies to any of an institution's third-party arrangements, including lending. This guidance expands upon the principles in that guidance by setting forth safety and soundness and consumer compliance measures FDIC-supervised institutions should follow when lending through a business relationship with a third party.

An institution's board of directors and senior management are ultimately responsible for managing activities conducted through third-party relationships, including lending relationships, and for identifying and controlling the risks arising from such relationships as if the activity were handled within the institution. The FDIC will evaluate lending activities conducted through third-party relationships as though the activities were performed by the institution itself. The institution, its board, and senior managers retain the ultimate responsibility to conduct lending activities in a safe and sound manner, in accordance with existing supervisory guidance, and in compliance with applicable laws and regulations.

A listing of applicable guidance, regulations, and laws are cited at the end of this guidance.[2] Management should consider the principles addressed in this guidance and ensure that appropriate procedures are in place, taking into account the type of lending activity, complexity, volume, and number of third-party lending relationships. Institutions that engage in new or significant lending activities through third parties will generally receive increased supervisory attention. Third-party lending arrangements will be considered significant if, for example, they have a material impact on revenues, expenses, or capital; involve large lending volumes in relation to the bank's balance sheet; involve multiple third parties; or present material risk of consumer harm.

Background

[1] For purposes of this guidance, the terms "lending" and "loan" include any credit or financing arrangement, even if the transaction is not categorized as a loan on the institution's balance sheet.

[2] This is not an all-inclusive list, and depending on the type of product, service or relationship, other guidance, regulations, or laws may apply.

Third-party lending is a lending arrangement that relies on a third party to perform a significant aspect of the lending process, such as some or all of the following: marketing; borrower solicitation; credit underwriting; loan pricing; loan origination; retail installment sales contract issuance; customer service; consumer disclosures; regulatory compliance; loan servicing; debt collection; and data collection, aggregation, or reporting.

Third-party lending arrangements may include the following:

- **Insured institutions originating loans <u>for third parties</u>** – In these situations, an insured institution typically serves as the originator for an entity that lacks the necessary licenses or charter to lend on its own behalf or seeks to take advantage of the institution's ability to export interest rates.[3] Often, the insured institution does not retain significant amounts of loan volume generated, but rather holds the loan for only a short period of time before selling it to the third party, which typically secures the ultimate funding source. In some of these arrangements, the loan volumes passing through insured institutions exceed by many multiples the bank's balance sheet.
- **Insured institutions originating loans <u>through third-party lenders</u> or <u>jointly with third-party lenders</u>** – In these arrangements, an insured institution relies on a third party to generate loan volume for the institution by authorizing the agent to offer loans on the institution's behalf. Loans generated through this model are typically retained by the insured institution, and in some situations, insured institutions may utilize multiple agents, sometimes numbering into the thousands and sometimes geographically dispersed. In other instances, third-party lenders and insured institutions act jointly to originate and fund credit.
- **Insured institutions originating loans <u>using platforms developed by third parties</u>** – In these situations, an insured institution relies on a third party to create and support a nearly end-to-end lending platform for the institution's use. Most often, loans generated through this model are retained by the bank

Potential Risks Arising from Third-Party Lending Relationships

As noted in the Third-Party Guidance, there are numerous risks that may arise or be heightened from a financial institution's use of third parties. The Third Party Guidance describes general risks associated with any type of third-party arrangement and the consequences that may occur from failure to adequately manage or mitigate these risks. Institutions should be aware of those risks as a baseline, but should also be aware of risks that are particularly associated with third-party lending programs. Not all of the following risks will be applicable to every third-party lending relationship and there may be other risks not described below.

[3] Federal law authorizes state-chartered depository institutions to charge interest on loans to out of state borrowers at rates authorized by the state where the financial institution is located, regardless of usury limitations imposed by the state laws of the borrower's residence. See Section 27 of the Federal Deposit Insurance Act, 12 U.S.C. § 1831d (enacted as section 521 of the Depository Institutions Deregulation and Monetary Control Act of 1980). However, courts are divided on whether third-parties may avail themselves of such preemption. See e.g., *CashCall, Inc v Morrisey*, Mo 12-1274, 2014 WL 2404300 (W Va. May 30, 2014).

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. As a core banking function, the use of third parties to perform functions related to lending or to offer products or services that do not help the institution achieve corporate strategic goals exposes the institution to strategic risk. For instance, the potential misalignment of incentives or goals between the institution and the third party partner may elevate strategic risk.

Operational Risk

Operational risk is the loss resulting from inadequate or failed internal processes, people, and systems or from external events. Third-party lending relationships integrate the internal processes of other organizations with the bank's processes and can increase the overall operational complexity. Due to the nature of many third-party lending relationships, key operational factors such as underwriting, servicing, or other customer interaction may be completed at another location and/or by employees not under the direct supervision of the insured institution.

Transaction Risk

Transaction risk arises from problems with service or product delivery. Particularly in situations where large volumes of loans are originated or multiple third parties or agents are involved, insured institutions can be significantly exposed to transaction and operational risks. Significant amounts of and/or growth in customers, transactions, and documents exposes insured institutions to heightened levels of concern regarding adequate safety and soundness and consumer protection compliance capacity, technology weaknesses, human error, weak controls, or fraud or other serious weaknesses at the third party, among other things.

Transaction risk can be particularly acute in situations involving multiple relationships where the third parties may have limited resources to ensure compliance with the institution's parameters, supervisory expectations and guidelines, and applicable regulations and laws. Transaction risk is also heightened when the third party itself relies on other third-party vendors as part of its business process. Transaction risk can also be associated with legal risks unique to third-party relationships. For example, insured institutions may incur liability in connection with joint activities or by operation of law that governs assignees of certain credit transactions.

Pipeline and Liquidity Risk

Pipeline risk relates to the risks associated with transactions failing to be consummated and funded as expected. Institutions originating loans through third-party arrangements in which the loans are expected to be sold, are subject to pipeline risk, and as a result, liquidity and funding risk, should the third party responsible for purchasing the loan production not be able to perform as agreed.

Model Risk

Model risk occurs when a financial model used to generate or value transactions or measure a firm's risks does not perform the tasks or capture the risks it was designed to or is used improperly in an institution's decision-making process. Some third-party lending relationships are heavily dependent on quantitative models developed by third parties, particularly in those arrangements in which institutions originate loans for third parties or use third party lending platforms. Model risk can be significant if a large portion of the third-party lending process is dependent upon models and/or if the models developed and used by the third party are not adequately understood by the insured institution's management. Insured institutions can also be exposed to increased compliance risk if models do not comply with consumer protection laws and regulations.

Credit Risk

Credit risk is the risk that a third party, or any other creditor necessary to the third-party relationship, in unable to meet the terms of the contractual arrangements with the insured institution or to otherwise perform as agreed. Institutions engaging in lending activities are exposed to credit risk, and the ability to manage credit risk can be more challenging when origination volumes are significant or there are numerous third-party relationships. These challenges can be exacerbated because incentives of third parties involved in lending may not be aligned with those of the institution. For example, often in third-party lending arrangements, third parties are paid fees for providing lending-related services regardless of transaction quality. Additionally, in other arrangements, third parties sometimes have an incentive to make or price loans in order to complete another transaction, such as a retail sale of a good or service, which may result in less attention to the quality of the loan. Certain loans may be underwritten off-site, increasing the risk that agents or employees of third-party lenders may misrepresent information about the loans or increase credit risk by failing to adhere to established underwriting guidelines.

Credit risk should not be disregarded if loans are sold, particularly if the institution is subject to repurchase requirements. Even where an insured institution properly seeks to mitigate the risks of third-party lending arrangements through contracts that provide indemnifications, parameters around representations and warranties, and/or limits on repurchases, such agreements do not insulate the institution from its ultimate responsibility to conduct lending activities in a safe and sound manner and in compliance with laws and regulations.

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. Compliance risks are heightened when an institution engages in third-party lending activities. These heightened risks exist throughout the life of the borrower's relationship with the lender and may relate to compliance with requirements with respect to lending activities.

Consumer Compliance Risk

Consumer compliance risk may arise in numerous areas related to lending activities, including fair lending; debt collection; credit reporting; privacy; and unfair and deceptive acts or practices, among others. Specific risks and the potential for consumer harm can be elevated in these relationships depending on the inherent risk in the product offered, the level of third-party involvement throughout the life of the customer relationship, the number of third parties utilized by the institution, the size and volume of third-party lending as part of the institution's lending activity, and the extent to which an institution has implemented an effective compliance management system that incorporates the activities of third parties.

Bank Secrecy Act/Anti-Money Laundering (BSA/AML)

Institutions that rely on a third party to conduct any aspect of BSA/AML, such as customer information collection, due diligence, and suspicious activity monitoring and reporting, may be exposed to increased compliance risk, as third parties may lack specialized BSA/AML expertise, staffing, training, structure, and systems to facilitate and ensure compliance.

Third-Party Lending Risk Management Program

As described in the Third-Party Guidance, the key to the effective use of a third party in any capacity, including third-party lending relationships, is for the financial institution's management to appropriately assess, measure, monitor, and control the risks associated with the relationship. Engaging in a third-party lending arrangement may enable the institution to achieve strategic or profitability goals, but reduces management's direct control. Therefore the use of third parties to engage in lending activities increases the need for strong risk management and oversight around the entire process, including a comprehensive compliance management system.

To this end, institutions should establish a third-party lending risk management program and policies prior to entering into any significant third-party lending relationships. The program and policies should be commensurate with the significance, complexity, risk profile, transaction volume, and number of third-party lending relationships. Moreover, institutions engaging in third-party lending activities need a process for evaluating and monitoring specific third-party relationships. This process is described in the Third-Party Guidance as comprising of four elements: (1) risk assessment, (2) due diligence in selecting a third party, (3) contract structuring and review, and (4) oversight.

<u>Developing a Third-Party Lending Risk Management Program</u>

Strategic Planning

Institutions should incorporate third-party lending activities into the strategic planning process and should establish clear risk tolerance limits around the size of the overall program based on appropriate objectives, projections, and assumptions. The institution should ensure it has the necessary management, staffing, and expertise to conduct the appropriate due diligence, manage,

and oversee the program and the third-party lending relationships. Strategic planning regarding third-party lending arrangements should also consider economic conditions, operational and informational technology capacity, risk-return tradeoffs, the need to establish an appropriate allowance for loan and lease losses, and capital support. Strategic planning should also incorporate back-up plans in the event that third-party lending arrangements do not go as planned.

Third-Party Lending Policies

Third-party lending program policies should be developed by management and approved by the institution's board, and should at a minimum:

- Establish limits as a percent of total capital for each third-party arrangement and for the program overall, relative to origination volumes, credit exposures (including pipeline risk), growth, loan types, and levels of credit quality (such as delinquency, losses, and charge-offs).
- Establish responsibilities, authorities, and approval requirements for selecting individual third-party lending relationships.
- Establish minimum performance standards for third parties; requirements for independent reviews of each third party; and a program for management oversight of each third-party arrangement.
- Establish monitoring, both for individual third parties and as part of the institution's overall lending activity, to identify, assess, and mitigate risks, such as fair lending.
- Establish reporting processes (including board reporting).
- Require access to data or other program information.
- Define permissible loan types.
- Establish credit underwriting, administration, and quality standards.
- Establish a consumer complaint process that provides for timely identification and resolution of complaints, complaint monitoring, and periodic reporting.
- Address capital and liquidity support and allowance for loan and lease loss considerations.
- Ensure the compliance officer has necessary authority, accountability, and resources; ensure that he or she has knowledge and understanding of relevant consumer protection laws and regulations that apply to the third-party lending arrangements.
- Maintain an adequate training program that incorporates laws, regulations, guidance, and policies and procedures and that the institution ensures appropriate training is provided to relevant third-party personnel.

<u>Elements for Evaluating and Monitoring Third-Party Relationships</u>

Risk Assessment

As discussed in the Third-Party Guidance, risk assessment is fundamental to the initial decision of whether to enter into individual third-party relationships. A risk assessment will inform the institution of the risks associated with providing credit through third parties so that the institution, in turn, can decide how it can mitigate such risk.

The risk assessment should ensure that the proposed third-party lending relationship fits within the institution's strategic plan and business model and that management has the requisite knowledge to analyze, and later oversee, the appropriateness of a particular third-party lending relationship. Management's ability to oversee third-party lending relationships can be particularly difficult when, for example, the institution originates large, rapidly growing lending volumes, or engages multiple, geographically dispersed third parties. Management should fully understand and assess the benefits, costs, and potential risks associated with the third-party relationship prior to entering into the relationship, and conduct a new risk assessment if a third party changes its operations or the institution's lending operations change over time.

Due Diligence and Ongoing Oversight

Management should conduct due diligence on each third-party lending relationship to identify the suitability of the relationship, including whether management will be able to appropriately oversee the relationship going forward. Comprehensive due diligence and oversight involves a review of all available information about a third party, focusing on the entity's policies and procedures, financial condition, its specific experience and quality of management, and the effectiveness of its operations and controls.

The scope of such reviews, and in the case of ongoing reviews, the frequency, should be commensurate with the risk of the relationship activities, and for significant arrangements, may need to be more frequent. For example, institutions originating loans for third parties in volumes that exceed the size of the institution's balance sheet by many multiples or relationships with large, or multiple, widely dispersed third parties, would be expected to oversee the third-party lending arrangements on an ongoing basis.

While an institution may hire another party to perform certain due diligence and oversight functions, doing so does not diminish its due diligence or oversight responsibilities. Due diligence and ongoing monitoring findings should be reported to the board. The following is a listing of minimum expectations for due diligence and oversight. Comprehensive due diligence involves a review of all available information related to the third party, so institutions should not limit due diligence and ongoing reviews to the items in the Third-Party Guidance or listed here:

- Policies and procedures;
- Credit quality of loans solicited or underwritten by the third party;
- System of internal controls and extent of internal and external audit;
- Knowledge and experience of management and staff, particularly firm principals;
- Repurchase activity and volume;
- Management information systems;
- Compliance management systems;
- Results of the institution's monitoring of its third party data;
- Consumer complaints received;
- Information security program to protect consumer information;
- Litigation or enforcement actions;

- Earnings strength and adequacy of capital; and
- Stability of funding sources and back-up sources of liquidity

Ongoing oversight should include an audit or other independent verification of third-party activities, including an assessment of the third party's compliance with policies, procedures, contracts, and guidance, regulations, and laws applicable to the activities it performs on the institution's behalf. Institutions should periodically test a sample of transactions and conduct site inspections to assess the adequacy and compliance of the third party's operations and to ensure the third party is conducting business in line with expectations and requirements. The audit/independent verification, transaction testing, and site inspection scope depends on the complexity, size, and risk profile of the third-party lending program and may need to be continuous for significant programs with large volumes and multiple third-party relationships. Findings should be reported to the board, and exceptions should be tracked through final remediation. Corrective action (including updates to the third party's policies and procedures, additional training, enhancements to the institution's monitoring and restitution) may be necessary. Depending on the type and level of risk posed by the third-party arrangement, institutions should consider establishing a mystery shopper program.

- Model Risk Management

Institutions need to understand models used by third parties in lending arrangements. Institutions should review model development documentation and independent model validation, ongoing monitoring, outcomes analysis, annual reviews, and audits prior to model use, and periodically thereafter based on the level of model reliance and model significance, to:

- Develop an understanding of the model's design, theory, logic, and methodologies;
- Assess data and model quality, conceptual soundness, and reliability;
- Determine that the model reflects the institution's underwriting standards or pricing policies;
- Ensure that models consider fluctuations in the economic cycles and are adjusted to account for other unexpected events; and
- Ensure the models are developed and operated in compliance with applicable consumer protection laws and regulations, including fair lending.

Such assessments should be performed by objective and independent personnel that are competent and have relevant technical knowledge and modeling skills. Additionally, institutions should assess the adequacy of the third party's model implementation, use, governance, policies, and controls.

- Vendors Used by Third Parties

The institution should assess the adequacy of the third party's vendor management or third-party risk management process. For material vendor relationships, the institution should review the third party's due diligence, risk assessment, and oversight. Risks related to the third party's use of vendors or other entities should be incorporated into the risk assessment of the third-party

relationship, and transaction testing and site visits of the third party's vendors should be considered, as appropriate, for large or significant vendors.

Contract Structuring and Review

As described in the Third-Party Guidance, third-party lending relationships and loan sale/purchase agreements should be governed by written contractual agreements that clearly establish the rights and responsibilities of each party to the contract. For third-party lending arrangements in particular:

- Indemnification, representations, warranties, and recourse terms should limit the institution's exposure and should not expose the institution to substantial risk.
- Legal counsel review should include an analysis of the program and agreements to identify legal risk and an opinion concerning any potential recourse to the institution.
- Agreements should not limit the institution's ability to sell loans to another entity if the third party is unable to purchase loans under the agreement.
- Termination rights should be sought for excessive risk exposure, material deterioration in the institution's or third party's financial condition, or if required by the state regulators or the FDIC.
- Contracts should provide the institution full discretion and authority to require the third party to implement policies and procedures for any function or activity it outsources to the third party or that are integral to joint activities with the third party.
- Contracts should allow the institution to have full access to any information or data necessary to perform its risk and compliance management responsibilities, including access to loan performance data, internal and external audits, and funding information.
- Establish protections for the institution due to a third party or subcontractor's negligence, such as insurance.

Supervisory Considerations for Third-Party Lending Relationships

The following are some of the supervisory considerations related to third-party lending relationships.

<u>Credit Underwriting and Administration</u>

Whether an institution is originating loans for a third party, through/jointly with a third party, or using platforms developed by a third party, credit underwriting and administration standards must be established by the institution, not the third party. Standards must comply with existing safety and soundness principles, guidelines, and regulations; be commensurate with the board's risk appetite and strategies; and be supported by adequate capital, funding sources, and an appropriately funded allowance for loan and lease losses. The institution should establish a process to ensure that loan approvals by the third party comply with the institution's standards. Institutions should ensure that pre-approved offers sent to potential borrowers are consistent with the institution's credit standards.

Management should establish ongoing monitoring of loans generated through/jointly with a third party or using platforms developed by a third party using key measures, such as production volumes and trends, approval rates, decline rates, losses, delinquencies, and collections. Such measures should be monitored by various segments to allow meaningful analysis of credit quality, such as by individual third parties, loan type, origination period or vintage, and credit grade or score bands. Performance should be compared to projections. The cause of significant variance should be determined.

Monitoring results should be used to assess whether underwriting standards are appropriate. If monitoring reflects significant credit deterioration, weaker than projected loan performance, or heightened losses, management should re-assess credit standards and document support for changes or lack thereof. Institutions should also periodically perform sensitivity analysis to assess how changes in credit or economic conditions will affect the portfolio. Loans sold should be included in performance monitoring or sensitivity analysis.

Loss Recognition

For loans generated through/jointly with a third party or using platforms developed by a third party, the Board and management are expected to identify adversely classified loans and promptly charge-off loans deemed uncollectible. For retail credits, adverse classifications and losses should be identified at least according to the parameters outlined in the *Uniform Retail Credit Classification and Account Management Policy*. If loans do not have a contractual due date, the institution should establish a delinquency calculation that reflects more traditional repayment terms.

Subprime Programs

If third-party lending arrangements include subprime lending programs, existing subprime guidance applies, including the interagency *Expanded Guidance for Subprime Lending Programs* ("Subprime Guidance") and the FDIC's *Guidelines for Payday Lending*, as appropriate. The Subprime Guidance applies to programs with aggregate credit exposure greater than or equal to 25% of tier 1 capital, but may also be applied to certain smaller subprime programs.[4] Because of the challenges in overseeing risks related to third-party lending and because the threshold is not meaningful when institutions sell the majority of loans after origination, the Subprime Guidance will be applied to all subprime programs in third-party lending arrangements, regardless of whether the threshold is met.

Bank-defined prime lending programs that allow credit underwriting standards with subprime credit characteristics are not eligible for the exclusion from the Subprime Guidance. Similarly, prime programs that do not consider credit criteria (such as delinquencies, bankruptcies, foreclosure, repossession, and charge-off) that are commonly considered to categorize subprime are also not eligible for exclusion from the Subprime Guidance. Institutions originating

[4] "The Agencies may also apply these guidelines to certain smaller subprime portfolios, such as those experiencing rapid growth or adverse performance trends, those administered by inexperienced management, and those with inadequate or weak controls." Expanded Guidance for Subprime Lending Programs, page 2.

subprime loans, including payday loans, should establish policy concentration limits, as a percentage of total capital.

Capital Adequacy

Institutions engaged in third-party lending arrangements should determine the amount and level of capital necessary to reflect the risk in the institution's third-party lending program. Capital assessments based on loan volume without consideration of loans originated and sold and associated risks are insufficient. Institutions engaging in significant third-party lending activities are expected to maintain capital well-above regulatory minimums. Institutions engaged in subprime third-party lending are expected to comply with the heightened capital requirements in the Subprime Guidance.

Liquidity

Institutions engaged in third-party lending arrangements should maintain appropriate liquidity to reflect the funding risk in the institution's third-party lending program. In particular, institutions that originate loans for third parties and rely on loan sales to the third party should assess concentrations in funding sources and have appropriate back-up funding arrangements to address pipeline risk. Additionally, institutions should conduct sensitivity analysis to determine the potential impact in the event of a delay or halt in loan sales.

If cash collateral funds are in place to mitigate liquidity and pipeline risk, the institution should document how that collateral level was deemed appropriate and how often the level is reassessed to ensure risk exposure does not increase to unacceptable levels. The institution should also be able to demonstrate that it has the ability to access the collateral if a third party fails to purchase loans pursuant to contract.

Profitability

Institutions should project and budget costs and earnings of each relationship and for the third-party lending program overall prior to entering into relationships and periodically thereafter. Monitoring should compare budget and projections to actual performance to evaluate profitability, which should be considered in decisions to maintain the relationship. Projections should be tested to consider changes in economic conditions, interest rates, investor demand, and borrower demand.

Institutions should monitor reliance on income, revenues, and fees from each arrangement and program overall. Cost to exit a relationship, including the cost to obtain replacement services, and the impact on the financial condition if earnings were to cease should be incorporated in the profitability analysis, with potential impact on capital incorporated into the capital analysis.

Institutions should demonstrate that the fees paid to or by the institution are supported and provide the institution with an acceptable risk-adjusted return.

Accounting and Allowance for Loan and Lease Losses

Institutions should report purchased interests in accordance with applicable generally accepted accounting principles. Financial reporting considerations include, but are not limited to: true loan sale treatment, residuals, loan sale commitments, valuations / mark to market accounting, credit enhancing representations and warranties, and bookkeeping accuracy between the third party and the institution. An appropriate allowance for loan and lease losses should be maintained.

Consumer Compliance

As with other types of third-party relationships, partnering with third-party lenders does not relieve the institution from compliance with applicable laws and regulations. The institution is ultimately responsible for ensuring all aspects of third-party lending activities are in compliance with consumer protection and fair lending requirements to the same extent as if the activities were handled within the institution itself. In addition, the institution should have systems in place to ensure third parties utilized by the institution have the appropriate authority to conduct business on behalf of the institution, such as appropriate licensure. An institution's compliance management system should be appropriate to the size, complexity, and scope of its third-party lending relationships to effectively address emerging issues and to proactively identify and address compliance deficiencies. Third parties that have direct contact with borrowers, develop customer-facing documents, or provide new, complex, or unique loan products require enhanced compliance-related due diligence and oversight by the institution to ensure areas of potential consumer harm are identified and mitigated. Institutions that conduct a significant volume of lending through dispersed networks of third parties should be particularly attuned to potential elevated fair lending risks, especially when the institution's program permits significant levels of discretion.

Bank Secrecy Act/Anti-Money Laundering (BSA/AML)

Similarly, partnering with third-party lenders does not relieve the institution from compliance with BSA/AML requirements. If the institution relies on a third party to perform BSA/AML functions on its behalf, the institution is ultimately responsible for that third party's compliance with the BSA/AML requirements. Institutions should have written agreements in place that clearly outline each party's obligations and establish adequate controls and review procedures.

Safeguarding Customer Information

Institutions engaged in third-party lending relationships must also ensure that customer information is safeguarded when held by third parties. Specifically, institutions retain the responsibility to ensure compliance with the interagency guidelines establishing standards for safeguarding customer information issued by the banking agencies pursuant to the Gramm-Leach–Bliley Act. The interagency guidelines, which appear in Appendix B to Part 364 of the FDIC Rules and Regulations, require institutions to implement a written information security program to protect the security, confidentiality, and integrity of customer information. The guidelines further require institutions to assess reasonably foreseeable internal and external threats that could result in unauthorized uses or destruction of customer information systems, and

to design a security program to control those risks. An institution's board of directors should approve the written program and oversee its implementation. Institutions engaged in third-party lending should establish written expectations, training and oversight measures to ensure that third parties are safeguarding customer information in accordance with the interagency guidelines and reporting any breaches to the institution to ensure proper and timely notification to customers.

Information Technology

Institutions should be in compliance with the information technology expectations for third-party arrangements (including the third party's subcontracting activities) established in the *FFIEC Information Technology Handbook, "Outsourcing Technology Services."*

Examination Procedures for Third-Party Lending Relationships

Examiners will assess third-party lending relationships in conjunction with this guidance, the Third-Party Guidance, and any other applicable guidance, regulations, and laws (see resource list at the end of this document for examples).

For institutions with significant third-party lending programs relationships, the examination cycle will be at least every 12 months and include concurrent risk management and consumer protection examinations. Risk management examinations will include information technology and BSA/AML examinations. More frequent examination activities, such as visitations or ongoing examinations should be performed if significant risk is identified, such as significant increases in origination volumes and/or number of third-party arrangements; the third-party arrangements are a material portion of the institution's operations and strategy; or material weaknesses in the management of the third-party relationships is identified or a significant risk management, financial, or operational weakness is noted in the third party itself. In such situations, additional ongoing off-site monitoring should also be performed, including periodic reports on volumes, third-party relationship changes, consumer complaint trends, and credit performance.

Examiners will conduct targeted examinations of significant third-party lending arrangements and may also conduct targeted examinations of other third parties where authorized. Reviews should be of sufficient scope and frequency to assess the level of risk posed to the institution by the third-party arrangement, whether the risk is appropriately managed by the institution, and whether the third party is appropriately implementing agreed-upon policies and procedures and is in compliance with guidance, regulations, and laws applicable to the activities it performs on the institution's behalf. Third-party lending examination activities would typically include, but not be limited to, a review of corporate governance; financial strength; compliance management system; credit underwriting and administration; model risk management; vendor management; internal controls; audit program; BSA/AML; safeguarding of customer information, information technology; consumer complaints; and litigation. In certain cases, examination activities will include targeted reviews of compliance with fair lending laws, such as when lending through a

dispersed network of third parties poses a heightened fair lending risk or when an institution is employing a model with untested or unproven inputs.

Reviews of third parties should also include transaction testing of individual loans to assess compliance with consumer compliance regulations, underwriting and loan administration guidelines, credit quality, appropriate treatment of loans under delinquency, and re-aging and cure programs. The sample size of individual credit testing should be meaningful, and underlying documents and data inputs (including automated system inputs) should be reviewed.

Findings of third party reviews will be reflected in the Report of Examination. When examiners determine that management of safety and soundness or compliance risks is deficient, they should criticize management and initiate corrective action. Weaknesses should be reflected in applicable component ratings, the Management rating, and the composite rating in accordance with the Uniform Financial Institutions Rating System. Corrective actions may include formal or informal enforcement action. When serious deficiencies exist, enforcement actions may instruct institutions to discontinue third party lending.

For questions about this guidance, institutions should contact their appropriate FDIC Regional Office.

Resources

(This is not an all-inclusive list. Depending upon the type of product, service, or relationship, a listed item may not apply and other guidance, regulations, or laws may apply.)

Guidance for Managing Third-Party Risk (Financial Institution Letter (FIL) 44-2008, June 6, 2008)

Safety and Soundness Standards (Section 39 of the Federal Deposit Insurance Act)

Interagency Guidelines Establishing Standards for Safety and Soundness (Appendix A to Part 364 of the FDIC Rules and Regulations)

Real Estate Lending Standards (Part 365 of the FDIC Rules and Regulations)

Uniform Retail Credit Classification and Account Management Policy (FIL-40-2000, June 29, 2000)

Interagency Guidance on Subprime Lending (FIL-20-99, March 4, 1999)

Expanded Guidance for Subprime Lending Programs (FIL-9-2001, January 31, 2001)

Statement on Subprime Mortgage Lending (FIL-62-2007, July 10, 2007)

Guidelines for Payday Lending (FIL-14-2005, March 1, 2005 (revised November 2015))

Policy Statement on Allowance for Loan and Lease Losses Methodologies and Documentation for Banks and Savings Institutions

Interagency Guidelines Establishing Information Security Standards (Appendix B to Part 364 of the FDIC Rules and Regulations)

Privacy of Consumer Financial Information (Part 332 of the FDIC Rules and Regulations)

FFIEC Information Technology Handbook, "Outsourcing Technology Services"

Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice (FIL-27-2005, April 1, 2005)

Policy Statement on Discrimination in Lending (April 15, 1994)

Interagency Guidance Regarding Unfair or Deceptive Credit Practices (FIL-44-2014, August 22, 2014)

Unfair or Deceptive Acts or Practices by State-Chartered Banks (FIL-26-2004, March 11, 2004)

Social Media: Consumer Compliance Risk Management Guidance (FIL-56-2013, December 11, 2013)

Interagency Guidance on Mortgage Servicing Practices Concerning Military Homeowners with Permanent Change of Station Orders (FIL-28-2012, June 21, 2012)

FDIC's Supervisory Policy on Predatory Lending (FIL-6-2007, January 22, 2007)

Advisory Statement on Encouraging Financial Institutions to Work with Student Loan Borrowers Experiencing Financial Difficulties (FIL-35-2013, August 1, 2013)

Office of the Comptroller of the Currency
U.S. Department of the Treasury

OCC BULLETIN 2017-21

Subject: Third-Party Relationships
Date: June 7, 2017

To: Chief Executive Officers and Chief Risk Officers of All National Banks and Federal Savings Associations, Technology Service Providers, Department and Division Heads, All Examining Personnel, and Other Interested Parties

Description: Frequently Asked Questions to Supplement OCC Bulletin 2013-29

Summary

The Office of the Comptroller of the Currency (OCC) is issuing frequently asked questions (FAQ) to supplement OCC Bulletin 2013-29, "Third-Party Relationships: Risk Management Guidance," issued October 30, 2013.

Note for Community Banks

This bulletin addresses questions from national banks and federal savings associations (collectively, banks) regarding guidance in OCC Bulletin 2013-29. This bulletin and OCC Bulletin 2013-29 are applicable to all banks..

1. What is a third-party relationship?

OCC Bulletin 2013-29 defines a third-party relationship as any business arrangement between the bank and another entity, by contract or otherwise. Third-party relationships include activities that involve outsourced products and services; use of outside consultants, networking arrangements, merchant payment processing services, and services provided by affiliates and subsidiaries; joint ventures; and other business arrangements in which a bank has an ongoing third-party relationship or may have responsibility for the associated records. Recently, many banks have developed relationships with financial technology (fintech) companies that involve some of these activities, including performing services or delivering products to a bank's customer base. If a fintech company performs services or delivers products on behalf of a bank or banks, the relationship meets the definition of a third-party relationship and the OCC would expect bank management to include the fintech company in the bank's third-party risk management process.

Bank management should conduct in-depth due diligence and ongoing monitoring of each of the bank's third-party service providers that support critical activities. The OCC realizes that although banks may want in-depth information, they may not receive all the information they seek on each critical third-party service provider, particularly from new companies. When a bank does not receive all the information it seeks about third-party service providers that support the bank's critical activities, the OCC expects the bank's board of directors and management to

- develop appropriate alternative ways to analyze these critical third-party service providers.
- establish risk-mitigating controls.

- be prepared to address interruptions in delivery (for example, use multiple payment systems, generators for power, and multiple telecommunications lines in and out of critical sites).
- make risk-based decisions that these critical third-party service providers are the best service providers available to the bank despite the fact that the bank cannot acquire all the information it wants.
- retain appropriate documentation of all their efforts to obtain information and related decisions.
- ensure that contracts meet the bank's needs.

2. OCC Bulletin 2013-29 defines third-party relationships very broadly and reads like it can apply to lower-risk relationships. How can a bank reduce its oversight costs for lower-risk relationships?

Not all third-party relationships present the same level of risk. The same relationship may present varying levels of risk across banks. Bank management should determine the risks associated with each third-party relationship and then determine how to adjust risk management practices for each relationship. The goal is for the bank's risk management practices for each relationship to be commensurate with the level of risk and complexity of the third-party relationship. This risk assessment should be periodically updated throughout the relationship. It should not be a one-time assessment conducted at the beginning of the relationship.

The OCC expects banks to perform due diligence and ongoing monitoring for all third-party relationships. The level of due diligence and ongoing monitoring, however, may differ for, and should be specific to, each third-party relationship. The level of due diligence and ongoing monitoring should be consistent with the level of risk and complexity posed by each third-party relationship. For critical activities, the OCC expects that due diligence and ongoing monitoring will be robust, comprehensive, and appropriately documented. Additionally, for activities that bank management determines to be low risk, management should follow the bank's board-established policies and procedures for due diligence and ongoing monitoring.

3. How should banks structure their third-party risk management process?

There is no one way for banks to structure their third-party risk management process. OCC Bulletin 2013-29 notes that the OCC expects banks to adopt an effective third-party risk management process commensurate with the level of risk and complexity of their third-party relationships. Some banks have dispersed accountability for their third-party risk management process among their business lines. Other banks have centralized the management of the process under their compliance, information security, procurement, or risk management functions. No matter where accountability resides, each applicable business line can provide valuable input into the third-party risk management process, for example, by completing risk assessments, reviewing due diligence questionnaires and documents, and evaluating the controls over the third-party relationship. Personnel in control functions such as audit, risk management, and compliance programs should be involved in the management of third-party relationships. However a bank structures its third-party risk management process, the board is responsible for overseeing the development of an effective third-party risk management process commensurate with the level of risk and complexity of the third-party relationships. Periodic board reporting is essential to ensure that board responsibilities are fulfilled.

4. When multiple banks use the same third-party service providers, can they collaborate[1] to meet expectations for managing third-party relationships specified in OCC Bulletin 2013-29?

If they are using the same service providers to secure or obtain like products or services, banks may collaborate[2] to meet certain expectations, such as performing the due diligence, contract negotiation, and ongoing monitoring responsibilities described in OCC Bulletin 2013-29. Like products and services may, however, present a different level of risk to each bank that uses those products or services, making collaboration a useful tool but insufficient to fully meet the bank's responsibilities under OCC Bulletin 2013-29. Collaboration can leverage resources by distributing costs across multiple banks. In addition, many banks that use like products and services from technology or other service providers may become members of user groups. Frequently, these user groups create the opportunity for banks, particularly community banks, to collaborate with their peers on innovative product ideas, enhancements to existing

products or services, and customer service and relationship management issues with the service providers. Banks that use a customized product or service may not, however, be able to use collaboration to fully meet their due diligence, contract negotiation, or ongoing responsibilities.

Banks may take advantage of various tools designed to help them evaluate the controls of third-party service providers. In general, these types of tools offer standardized approaches to perform due diligence and ongoing monitoring of third-party service providers by having participating third parties complete common security, privacy, and business resiliency control assessment questionnaires. After third parties complete the questionnaires, the results can be shared with numerous banks and other clients. Collaboration can result in increased negotiating power and lower costs to banks during the contract negotiation phase of the risk management life cycle.

Some community banks have joined an alliance to create a standardized contract with their common third-party service providers and improve negotiating power.

5. When collaborating to meet responsibilities for managing a relationship with a common third-party service provider, what are some of the responsibilities that each bank still needs to undertake individually to meet the expectations in OCC Bulletin 2013-29?

While collaborative arrangements can assist banks with their responsibilities in the life cycle phases for third-party risk management, each individual bank should have its own effective third-party risk management process tailored to each bank's specific needs. Some individual bank-specific responsibilities include defining the requirements for planning and termination (e.g., plans to manage the third-party service provider relationship and development of contingency plans in response to termination of service), as well as

- integrating the use of product and delivery channels into the bank's strategic planning process and ensuring consistency with the bank's internal controls, corporate governance, business plan, and risk appetite.
- assessing the quantity of risk posed to the bank through the third-party service provider and the ability of the bank to monitor and control the risk.
- implementing information technology controls at the bank.
- ongoing benchmarking of service provider performance against the contract or service-level agreement.
- evaluating the third party's fee structure to determine if it creates incentives that encourage inappropriate risk taking.
- monitoring the third party's actions on behalf of the bank for compliance with applicable laws and regulations.
- monitoring the third party's disaster recovery and business continuity time frames for resuming activities and recovering data for consistency with the bank's disaster recovery and business continuity plans.

6. What collaboration opportunities exist to address cyber threats to banks as well as to their third-party relationships?

Banks may engage with a number of information-sharing organizations to better understand cyber threats to their own institutions as well as to the third parties with whom they have relationships. Banks participating in information-sharing forums have improved their ability to identify attack tactics and successfully mitigate cyber attacks on their systems. Banks may use the Financial Services Information Sharing and Analysis Center (FS-ISAC), the U.S. Computer Emergency Readiness Team (US-CERT), InfraGard, and other information-sharing organizations to monitor cyber threats and vulnerabilities and to enhance their risk management and internal controls. Banks also may use the FS-ISAC to share information with other banks.

7. Is a fintech company arrangement considered a critical activity?

A bank's relationship with a fintech company may or may not involve critical bank activities, depending on a number of factors. OCC Bulletin 2013-29 provides criteria that a bank's board and management may use to determine what critical activities are. It is up to each bank's board and management to identify the

critical activities of the bank and the third-party relationships related to these critical activities. The board (or committees thereof) should approve the policies and procedures that address how critical activities are identified. Under OCC Bulletin 2013-29, critical activities can include significant bank functions (e.g., payments, clearing, settlements, and custody), significant shared services (e.g., information technology), or other activities that

- could cause the bank to face significant risk if a third party fails to meet expectations.
- could have significant bank customer impact.
- require significant investment in resources to implement third-party relationships and manage risks.
- could have major impact on bank operations if the bank has to find an alternative third party or if the outsourced activities have to be brought in-house.

The OCC expects banks to have more comprehensive and rigorous management of third-party relationships that involve critical activities.

8. Can a bank engage with a start-up fintech company with limited financial information?

OCC Bulletin 2013-29 states that banks should consider the financial condition of their third parties during the due diligence stage of the life cycle before the banks have selected or entered into contracts or relationships with third parties. In assessing the financial condition of a start-up or less established fintech company, the bank may consider a company's access to funds, its funding sources, earnings, net cash flow, expected growth, projected borrowing capacity, and other factors that may affect the third party's overall financial stability. Assessing changes to the financial condition of third parties is an expectation of the ongoing monitoring stage of the life cycle. Because it may be receiving limited financial information, the bank should have appropriate contingency plans in case the start-up fintech company experiences a business interruption, fails, or declares bankruptcy and is unable to perform the agreed-upon activities or services.

Some banks have expressed confusion about whether third-party service providers need to meet a bank's credit underwriting guidelines. OCC Bulletin 2013-29 states that depending on the significance of the third-party relationship, a bank's analysis of a third party's financial condition may be as comprehensive as if the bank were extending credit to the third-party service provider. This statement may have been misunderstood as meaning a bank may not enter into relationships with third parties that do not meet the bank's lending criteria. There is no such requirement or expectation in OCC Bulletin 2013-29.

9. How can a bank offer products or services to underbanked or underserved segments of the population through a third-party relationship with a fintech company?

Banks have collaborated with fintech companies in several ways to help meet the banking needs of underbanked or underserved consumers. Banks may partner with fintech companies to offer savings, credit, financial planning, or payments in an effort to increase consumer access. In some instances, banks serve only as facilitators for the fintech companies' products or services with one of the products or services coming from the banks. For example, several banks have partnered with fintech companies to establish dedicated interactive kiosks or automated teller machines (ATM) with video services that enable the consumer to speak directly to a bank teller. Frequently, these interactive kiosks or ATMs are installed in retail stores, senior community centers, or other locations that do not have branches to serve the community. Some fintech companies offer other ways for banks to partner with them. For example, a bank's customers can link his or her savings account with the fintech company's application, which can offer incentives to the bank's customers to save for short-term emergencies or achieve specific savings goals.

In these examples, the fintech company is considered to have a third-party relationship with the bank that falls under the scope of OCC Bulletin 2013-29.

10. What should a bank consider when entering a marketplace lending arrangement with nonbank entities?

When engaging in marketplace lending activities, a bank's board and management should understand the relationships among the bank, the marketplace lender, and the borrowers; fully understand the legal, strategic, reputation, operational, and other risks that these arrangements pose; and evaluate the marketplace lender's practices for compliance with applicable laws and regulations. As with any third-party relationship, management at banks involved with marketplace lenders should ensure the risk exposure is consistent with their boards' strategic goals, risk appetite, and safety and soundness objectives. In addition, boards should adopt appropriate policies, inclusive of concentration limitations, before beginning business relationships with marketplace lenders.

Banks should have the appropriate personnel, processes, and systems so that they can effectively monitor and control the risks inherent within the marketplace lending relationship. Risks include reputation, credit, concentrations, compliance, market, liquidity, and operational risks. For credit risk management, for example, banks should have adequate loan underwriting guidelines, and management should ensure that loans are underwritten to these guidelines. For compliance risk management, banks should not originate or support marketplace lenders that have inadequate compliance management processes and should monitor the marketplace lenders to ensure that they appropriately implement applicable consumer protection laws, regulations, and guidance. When banks enter into marketplace lending or servicing arrangements, the banks' customers may associate the marketplace lenders' products with those of the banks, thereby introducing reputation risk if the products underperform or harm customers. Also, operational risk can increase quickly if the operational processes of the banks and the marketplace lenders do not include appropriate limits and controls, such as contractually agreed-to loan volume limits and proper underwriting.

To address these risks, banks' due diligence of marketplace lenders should include consulting with the banks' appropriate business units, such as credit, compliance, finance, audit, operations, accounting, legal, and information technology. Contracts or other governing documents should lay out the terms of service-level agreements and contractual obligations. Subsequent significant contractual changes should prompt reevaluation of bank policies, processes, and risk management practices.

11. Does OCC Bulletin 2013-29 apply when a bank engages a third party to provide bank customers the ability to make mobile payments using their bank accounts, including debit and credit cards?

When using third-party service providers in mobile payment environments, banks are expected to act in a manner consistent with OCC Bulletin 2013-29. Banks often enter into business arrangements with third-party service providers to provide software and licenses in mobile payment environments. These third-party service providers also provide assistance to the banks and the banks' customers (for example, payment authentication, delivering payment account information to customers' mobile devices, assisting card networks in processing payment transactions, developing or managing mobile software (apps) or hardware, managing back-end servers, or deactivating stolen mobile phones).

Many bank customers expect to use transaction accounts and credit, debit, or prepaid cards issued by their banks in mobile payment environments. Because almost all banks issue debit cards and offer transaction accounts, banks frequently participate in mobile payment environments even if they do not issue credit cards. Banks should work with mobile payment providers to establish processes for authenticating enrollment of customers' account information that the customers provide to the mobile payment providers.

12. May a community bank outsource the development, maintenance, monitoring, and compliance responsibilities of its compliance management system?

Banks may outsource some or all aspects of their compliance management systems to third parties, so long as banks monitor and ensure that third parties comply with current and subsequent changes to consumer laws and regulations. Some banks outsource maintenance or monitoring or use third parties to automate data collection and management processes (for example, to file compliance reports under the Bank Secrecy Act or for mortgage loan application processing or disclosures). The OCC expects all banks to develop and maintain an effective compliance management system and provide fair access to financial services, ensure fair treatment of customers, and comply with consumer protection laws and regulations.

Strong compliance management systems include appropriate policies, procedures, practices, training, internal controls, and audit systems to manage and monitor compliance processes as well as a commitment of appropriate compliance resources.

13. Can banks obtain access to interagency technology service providers' (TSP) reports of examination?

TSP reports of examination[3] are available only to banks that have contractual relationships with the TSPs at the time of the examination. Because the OCC's (and other federal banking regulators') statutory authority is to examine a TSP that enters into a contractual relationship with a regulated financial institution, the OCC (and other federal banking regulators) cannot provide a copy of a TSP's report of examination to financial institutions that are either considering outsourcing activities to the examined TSP or that enter into a contract after the date of examination.

Banks can request TSP reports of examination through the banks' respective OCC supervisory office. TSP reports of examination are provided on a request basis. The OCC may, however, proactively distribute TSP reports of examination in certain situations because of significant concerns or other findings to banks with contractual relationships with that particular TSP.

Although a bank may not share a TSP report of examination or the contents therein with other banks, a bank that has not contracted with a particular TSP may seek information from other banks with information or experience with a particular TSP as well as information from the TSP to meet the bank's due diligence responsibilities.

14. Can a bank rely on a third party's Service Organization Control (SOC) report, prepared in accordance with the American Institute of Certified Public Accountants Statement on Standards for Attestation Engagements No. 18 (SSAE 18)?

In meeting its due diligence and ongoing monitoring responsibilities, a bank may review a third party's SOC report prepared in accordance with SSAE 18 to evaluate the effectiveness of the third party's risk management program, including policies, processes, and internal controls.[4] If a third party uses subcontractors (also referred to as fourth parties), a bank may find the third party's SSAE 18 report particularly useful, as SSAE 18 requires the auditor to determine and report on the effectiveness of controls the third party has implemented to monitor the controls of the subcontractor. In other words, the SSAE 18 report will address the question as to whether the third party has effective oversight of its subcontractors. A bank should consider whether an SSAE 18 report contains sufficient information and is sufficient in scope to assess the third party's risk environment or whether additional audit or review is required for the bank to properly assess the third party's control environment.

Further Information

The OCC encourages banks to contact their assigned local field office portfolio manager, assistant deputy comptroller, or appropriate large bank supervision staff members to discuss products and services involving third parties they are considering or to better understand how to meet their responsibilities for managing third-party relationships under OCC Bulletin 2013-29.

For questions regarding this bulletin or OCC Bulletin 2013-29, please contact Judi McCormick, Governance and Operational Risk Policy Analyst, Operational Risk Policy Division, at (202) 649-6550. The OCC intends to review banks' questions on OCC Bulletin 2013-29 from time to time and issue future FAQs or other guidance when it deems necessary.

Bethany A. Dugan
Deputy Comptroller for Operational Risk

---

[1] Refer to OCC News Release 2015-1, "Collaboration Can Facilitate Community Banks Competitiveness, OCC Says," January 13, 2015.

[2] Any collaborative activities among banks must comply with antitrust laws. Refer to the Federal Trade Commission and U.S. Department of Justice's "Antitrust Guidelines for Collaborations Among Competitors."

[3] The OCC conducts examinations of services provided by significant TSPs based on authorities granted by the Bank Service Company Act, 12 USC 1867. These examinations typically are conducted in coordination with the Board of Governors of the Federal Reserve Board, Federal Deposit Insurance Corporation, and other banking agencies with similar authorities. The scope of examinations focus on the services provided and key technology and operational controls communicated in the *FFIEC Information Technology Examination Handbook* and other regulatory guidance.

[4] As of May 2017, SSAE 18 replaced SSAE 16 for SOC 1 engagements.