Articles
June 01, 2023
Final Interagency Third-Party Risk Management Guidance Issued on June 6, 2023: Implications for Banks and FinTech Companies

There is an adage among regulators, "same risks, same rules" or "leveling up," and on June 6 the Office of the Comptroller of the Currency (OCC), Board of Governors of the Federal Reserve System (FRB), and Federal Deposit Insurance Corporation (FDIC) (together, the "Agencies") issued final interagency guidance on managing the risks associated with third-party relationships (Final Guidance).

The Final Guidance is an example of regulatory risk management and related expectations being applied to third parties through their affiliation with regulated banking organizations. Third-party relationships are proliferating, and they offer banking organizations significant benefits, such as access to new technologies, human capital, delivery channels, products, services, and markets. Some of the services being offered include innovative payment systems and processes, mobile platforms, the use of machine learning and artificial intelligence, and what has come to be known as "banking as a service" (BaaS). These relationships, however, create additional risks, and in addition to examining these operations within a banking organization, when circumstances warrant, the Agencies have the legal authority under the Bank Service Company Act (BSCA) to directly examine the operations of the third party concerning the services that it performs on a banking organization's behalf. As a result, third parties and financial technology (FinTech) companies need to understand their roles as well as their potential liabilities in their relationships with banking organizations and maintain strong risk management processes when initiating, forming, and continuing these relationships.

Below we provide a summary of the Final Guidance and analyze the key issues raised by it, and we provide some considerations as to the practical implications these revisions to the Final Guidance may have for banking organizations and FinTech companies.

Background

The Agencies began this project in July 2021 when they issued a proposal and request for public comment that used the OCC's third-party risk management guidance and the OCC's frequently asked questions (FAQs) as the template for soliciting input. Although each of the Agencies had previously issued guidance for their respective supervised banking organizations to address appropriate risk management practices for third-party relationships, the Final Guidance is most consistent with the OCC's previous guidance as it was the template selected by the Agencies in the comment phase. The Final Guidance effectively modified the OCC template to incorporate broader principles and best practices from across the Agencies into a set of risk-based principles. The Agencies will also be issuing additional resources in this area for smaller and less complex banking organizations.

There have been several significant events since the proposal was published that likely affected both the scope and timing of the Final Guidance, including:

- the so-called cryptocurrency winter that led to two unprecedented bank runs resulting in failures and the Agencies' statements relating to cryptocurrency and liquidity risks;
- the U.S. Department of the Treasury report, The Financial Services Sector's Adoption of Cloud Services, which highlighted some of the practices and the challenges;
- the Department of the Treasury report, Illicit Finance Risk Assessment on Decentralized Finance;
- the growth and risks in open banking and sharing customer data that was recently the focus of a speech by the acting comptroller of the currency;
- enforcement actions by the OCC and the FDIC that were specific to third-party risk management involving small community banks; and
- revisions to the OCC's enforcement policy to specifically address persistent weaknesses in large banks and complex banking structures, including those with significant third-party relationships.

Summary Observations

- The Final Guidance is welcome news for both the banking industry and the financial services industry more broadly, as the Agencies will be on the same page and applying the same supervisory standards in this important area. The structure and framework of the Final Guidance has not changed significantly from the previous OCC guidance, and there is more granularity and comprehensive information within each topical area.
- To the extent that banking organizations developed their third-party risk management programs against the previous guidance, these programs will need to be adjusted. Some notable changes in the Final Guidance include the use of a comprehensive inventory of third-party relationships, the elimination of the term "critical subcontractor" and oversight related to subcontractors, specific corporate governance requirements, numerous references to a banking organization's risk appetite, and collaboration and reliance on others for monitoring and due diligence.
- Nonbank relationships with banking organizations and involvement in banking activities is very clearly on the regulatory radar. Infrastructure providers and nonbank partners, including cloud services and FinTech companies, should expect more scrutiny of their services from their banking organization partners and potentially from the Agencies as well if they are key providers of critical support to the industry.
- The Final Guidance is just the latest in a series of moves from the U.S. government focused on identifying and mitigating potential risks in the financial system that arise from nonbank interactions that include the 2021 Computer-Security Incident Notification Rule, the Department of the Treasury Report on the Financial Services Sector's Adoption of Cloud Services, and the Financial Stability Oversight Council's recent proposal on the Authority to Require Supervision and Regulation of Certain Nonbank Financial Companies.
- The Final Guidance may create unrealistic expectations for small community banks with limited resources.

The Final Guidance

The Final Guidance supersedes the Agencies' previous third-party risk management guidance, including the OCC's FAQs, and broadly applies to any business arrangement between a banking organization and another entity, by contract or otherwise, and the arrangement can exist despite a lack of a contract or renumeration. The term "business relationship" is interpreted by the Agencies broadly and is synonymous with the term "third-party relationship." The Final Guidance notes that these relationships have evolved—and may continue to evolve—over time to encompass a large range of activities and justified the use of broad terminology. These relationships can include, but are not limited to, customer relationships, vendor relationships, outsourced services, independent consultants, referral arrangements, merchant payment processing services, services provided by affiliates and subsidiaries, and joint ventures. The Agencies do not discuss or provide any examples of what may not constitute a "business arrangement," but they expressly point out that some customer relationships could also constitute business relationships, thus clarifying the position taken by the OCC in its previous guidance and addressing certain BaaS arrangements involving customers of the third party that may not be customers of the banking organization. Where the third-party relationship involves the provision of products or services to, or other interaction with, customers, the banking organization and the third party may have varying degrees of interaction with those customers. Relationships that are between only banking organizations and their direct customers of traditional bank products and services (such as deposit accounts or retail or commercial loans) would not be addressed in a third-party risk management framework and are covered by the various risk management processes and rules that apply to traditional lending and deposit relationships.

Risk Management

The Final Guidance is risk-based. The use of third parties can reduce a banking organization's direct control over activities and may introduce new risks or increase existing risks, such as operational, compliance, and strategic risks. Increased risk arises from greater operational or technological complexity, newer or different types of relationships, or potential poor performance by the third party. Effective risk management requires the application of a sound methodology to designate which activities and third-party relationships receive more comprehensive oversight. In this regard, "critical activities" include those activities that could:

- Cause a banking organization to face significant risk if the third party fails to meet expectations;
- Have significant customer impacts; or
- Have a significant impact on a banking organization's financial condition or operations.

The Final Guidance acknowledges that an activity that is critical for one bank may not be critical for another, making it incumbent on each banking organization to identify its critical activities as well as any third-party relationships that support those critical activities. Some banks may assign a criticality or risk level to each third-party relationship, whereas others may identify critical activities and those third parties that support them. The Final Guidance references risk management principles that include: (i) an inventory of all third-party relationships with periodic risk assessments over time, and (ii) an analysis of risks associated with each third-party relationship (quantity of risk or inherent risk) and a risk management process commensurate with the risks (quality of risk management or controls) that includes the identification of residual risks and their consistency with the banking organization's risk appetite. Banking organizations should develop a sound methodology to identify activities and relationships that receive more oversight.

The term "risk appetite" is peppered throughout the Final Guidance, suggesting that banking organizations of any size and complexity should consider more comprehensive risk limits and metrics relating to their third-party risk management. Risk appetite generally means a set of objectives and risk parameters within which senior management of the banking organization should operate. Certain large banking organizations with total

consolidated assets in excess of $50 billion are required or expected to have a more comprehensive risk management framework that includes a written risk appetite statement from the board of directors. Many smaller community banks may not have formalized risk appetite statements but instead may establish appropriate metrics for measuring and monitoring key risks, and performance and risk reports are developed to enable the board of directors to monitor risk positions in relation to the risk assessment, risk limits, and risk parameters. Banking organizations should consider revisiting their overall risk management framework or risk appetite and ensure that any third-party relationships supporting higher-risk activities, including critical activities, are appropriately addressed. Smaller banking organizations with significant third-party relationships may find it useful to develop a written risk appetite statement for the purpose of third-party risk management. The Heightened Standards Rule issued by the OCC defines a risk appetite statement and provides some insights for its use and development that may be useful when considering or developing a risk appetite statement specific to third-party risk management.

Third-Party Relationship Life Cycle

The Final Guidance is structured similarly to each of the Agencies' prior guidance documents, focusing on identifying the risks, conducting due diligence and selection, structuring contracts, and ongoing review and oversight. The OCC's previous guidance incorporated these concepts into a so-called third-party relationship cycle, and this framework was adopted in the Final Guidance. Banking organizations should ensure that staff or external firms have the knowledge and skills to effectively manage each stage of the life cycle, especially in the skill areas relating to compliance (consumer and anti-money laundering), risk management, technology, and law.

Planning. The first stage in the third-party relationship life cycle is the planning stage, and a banking organization should consider:

- The strategic purpose of the business arrangement and how it aligns with the banking organization's goals, objectives, risk appetite, risk profile, and broader corporate policies;
- The risks and benefits to the arrangement;
- The nature of the business relationship, such as the volume of activity, use of subcontractors, technology needed, customer interactions, and use of foreign entities;
- Direct and indirect costs;
- The impact of the relationship on employees and any dual employees, especially when the outsourcing activities are currently conducted internally;
- Information security and physical security implications;
- How to select, assess, and oversee the third party, including monitoring for compliance with applicable laws, regulations, and contractual provisions and remediation of compliance issues that may arise;
- The ability to provide adequate oversight and management of the relationship on an ongoing basis; and
- Contingency planning.

Selection and Due Diligence. The second stage in the third-party relationship life cycle is the due diligence stage, and due diligence of a third-party relationship should be commensurate with the risk and complexity of the relationship. A banking organization needs to individually evaluate the risks presented by each third-party relationship and not, for example, reduce due diligence based solely on a third party's entity. The Final Guidance provides several factors to consider as part of due diligence, depending on the degree of risk and complexity of the relationship, including:

- Review of the third party's strategies and goals including mergers, acquisitions, and employment practices;
- Review of legal and regulatory compliance, including ownership structure, Office of Foreign Assets Control (OFAC) compliance, and responsiveness to other compliance issues and processes to mitigate consumer harm;
- Financial condition based on a review of available information;

- Business experience including depth of resources, experience, and addressing complaints;
- Qualifications and backgrounds of principals and key personnel, including whether the third-party conducts background checks and has suitability requirements;
- Risk management, including policies, processes, and internal controls;
- Information security, including access to a banking organization's systems and the third party's security program;
- Management of information systems that will be supporting the activity;
- Operational resilience and ability to recover from any disruptions;
- Incident reporting to ensure that the processes meet the banking organization's regulatory requirements set forth in the Computer-Security Incident Notification Rule;
- Physical security and environmental controls to protect the safety and security of employees and customers;
- Reliance on subcontractors and the volume and types of subcontractor activity;
- Insurance coverage and the extent to which potential losses are mitigated; and
- Contractual arrangements and commitments the third party may have with other parties.

In a nod to smaller banking organizations, the Final Guidance notes that a banking organization may collaborate with and use the services of industry utilities or consortiums, consult with other organizations, or engage in joint efforts to supplement its due diligence and effective risk management processes. Also, when a banking organization is unable to obtain the desired due diligence information, alternative processes should be developed that could include increased controls or monitoring of the relationship.

Contract Negotiation. The third stage in the third-party relationship life cycle is the contract negotiation stage. The banking organization should determine whether a written contract is needed and can meet its business goals and risk management needs. The Final Guidance provides specific factors to consider when negotiating contracts, including:

- The nature and scope of the arrangement that clearly identifies rights and responsibilities;
- Performance measures or benchmarks to assist in evaluating performance;
- Responsibilities for providing, receiving, and retaining information;
- Right to audit and require remediation;
- Responsibility for compliance with applicable laws and regulations;
- Costs and compensation to reduce disputes and ensure consistency with sound practices;
- Ownership and license to prevent disputes over proprietary information;
- Confidentiality and integrity due to increased risks related to nonpublic information and access to infrastructure;
- Operational resilience and business continuity in the event of problems affecting the third party's operations that also address backup systems;
- Indemnification and limits on liability to reduce liability for the banking organization;
- Insurance against losses including specific insurance maintained by the third party;
- Dispute resolution to resolve problems expeditiously;
- Customer complaints handled appropriately;
- Subcontracting arrangements that include notification to the banking organization, as appropriate;
- Foreign-based third parties and choice of law provisions and privacy laws;
- Default and termination provisions to protect the ability of the banking organization to change third parties when appropriate; and
- Regulation and supervision of the third party under the BSCA.

The Final Guidance also addresses situations where the banking organization has limited negotiating power. In these situations, a banking organization should understand resulting limitations and whether: (i) the contract can

still meet its needs, (ii) the residual risks are acceptable and within the risk appetite, (iii) to employ others, and (iv) to bring the activity in-house.

Ongoing Monitoring. The fourth stage in the third-party relationship life cycle involves ongoing monitoring of the relationship. This is arguably the most important aspect of the third-party relationship life cycle. Banking organizations cannot simply rely on the third-party service provider contractual provisions and representations but must affirmatively and continuously verify that the third party is performing as expected. The Agencies do not encourage any specific approach to ongoing monitoring and note that monitoring should occur throughout the duration of the relationship and be commensurate with the level of risk to confirm the quality and sustainability of a third party's controls and its ability to meet contractual obligations, escalate significant issues or concerns, and respond appropriately. Examples of typical monitoring activities provided include reports, site visits, and testing. Ongoing factors for banking organizations to consider when conducting ongoing monitoring include:

- The overall effectiveness of the relationship and consistency with strategic goals, business objectives, risk appetite, risk profile, and broader corporate policies;
- Changes to the third party's business strategy and agreements with other entities that may pose increased risks or impact its ability to meet contractual obligations;
- Changes in the third party's financial condition; changes to insurance coverage; relevant audits, testing results, and other reports; and ongoing compliance with applicable laws;
- Changes in key personnel involved in the activity to be performed by the third party;
- Reliance on and exposure to subcontractors;
- Training provided to employees of the banking organization and the third party;
- Response to changing threats and new vulnerabilities;
- Maintenance of confidentiality, availability, and integrity of the banking organization's systems, information and data, incident response, business continuity, and resumption plans;
- External factors that could affect performance (changing laws or economic conditions); and
- The volume, nature, and trends of customer complaints and the third party's responses and resulting remediation.

The Final Guidance also notes that banking organizations may engage external resources, refer to conformity assessments or certifications, or collaborate when performing ongoing monitoring.

Termination. The final stage of the third-party relationship life cycle addresses the termination of the relationship. The Final Guidance provides that, depending on the degree of risk and complexity of the third-party relationship, a banking organization typically considers several factors when terminating a third-party relationship, including options for effective transition of services, costs and fees, risks associated with data retention and destruction, information system connections and access control, and handling of joint intellectual property. If they are bringing the activities in-house, then banking organizations should consider their relevant capabilities and resources and the time frame required while still managing the legal, regulatory, customer, and other impacts that may arise.

Governance

In light of recent events, strong corporate governance has become a priority for the Agencies as well as a focus of the U.S. Congress, which is considering legislation (S.2190 RECOUP Act) in this area that will impact banking organizations. Consistent with this focus, the Final Guidance provides detailed instructions for strong governance, highlights both centralized and decentralized (business line) governance processes, and addresses oversight, independent reviews, and reporting based on risks and complexity as follows:

Oversight and Accountability. The Final Guidance sets forth the respective roles of the board of directors and senior management. The banking organization's board of directors has ultimate responsibility for providing oversight for third-party risk management and holding management accountable. The board of directors should provide clear guidance regarding acceptable risk appetite, approve appropriate policies, and ensure that the appropriate procedures and practices have been established. Management should develop and implement third-party risk management policies, procedures, and practices commensurate with the banking organization's risk appetite and the level of risk and complexity of its third-party relationships.

Independent Reviews. The Final Guidance addresses the importance of independent reviews to assess the adequacy of its third-party risk management processes. Banking organizations should promptly remediate and escalate identified concerns to the board of directors, as appropriate. These reviews should consider factors that include: (i) whether the third-party relationships align with the business strategy and internal policies, procedures, and standards; (ii) whether risks are identified, measured, monitored, and controlled; (iii) whether processes and controls are designed and operating effectively; (iv) whether appropriate staffing and expertise are engaged throughout the risk management life cycle; and (v) whether conflicts of interest are avoided or eliminated when selecting and overseeing third parties.

Documentation and Reporting. The Agencies stress that it is important for banking organizations to properly document and report on their third-party risk management processes and specific relationships throughout their life cycle. This includes maintaining an inventory of third-party relationships, customer complaints, and reports of service disruptions, security breaches, or other events that may pose a material risk to the banking organization.

Supervisory Reviews of Third-Party Relationships

Each of the Agencies will review its supervised banking organizations' risk management of third-party relationships as part of its standard supervisory processes to determine whether activities are conducted in a safe and sound manner and in compliance with applicable laws and regulations. The scope of these reviews will depend on the degree of risk and the complexity associated with banking organizations' activities and third-party relationships. The Agencies note that any examples in the Final Guidance are illustrative, not required, and that the Final Guidance should not be used as a check-the-box approach toward compliance by auditors or examiners. Each of the Agencies may use its legal authority set forth in the BSCA to examine functions or operations that a third party performs on a banking organization's behalf. These examinations may evaluate the third party's ability to fulfill its obligations in a safe and sound manner and comply with applicable laws and regulations, including those designed to protect consumers and to provide fair access to financial services. The Agencies highlight that the Final Guidance is guidance only, not a statute or regulation, and it is meant to clarify the Agencies' position, but it will not be enforced as a regulatory requirement beyond the normal role of guidance in the supervisory process. However, the Agencies make clear that they may pursue corrective measures, including enforcement actions, when necessary to address violations of laws and regulations or unsafe and unsound banking practices by the banking organization or its third party in situations where the underlying activities are problematic.

Key Takeaways for Banking Organizations

All banking organizations will need to "level up" their third-party risk management processes due to the changes implemented in the Final Guidance, depending on the banking organization's individual circumstances and degree of third-party risk. Some key changes from the Agencies' previous guidance are as follows:

- The use of a comprehensive inventory of third-party relationships;

- A customer relationship may be a "business arrangement";
- The elimination of the term "critical subcontractor";
- Oversight related to subcontractors;
- Numerous references to a banking organization's risk appetite and the implications for the establishment of risk limits and metrics or a written risk appetite statement;
- Collaboration and reliance for conducting ongoing monitoring and due diligence; and
- Fair and equitable treatment of consumers.

These are the most significant changes that likely impact existing third-party risk management policies, procedures, and processes and should be closely evaluated by banking organizations and third parties, as appropriate.

As a first step, banking organizations will need to evaluate their inventory of third-party relationships and ensure that it is comprehensive in scope and encompasses all business arrangements, including those with affiliates and certain customers, as appropriate. As a second step, banking organizations should conduct a review of the risks presented by these relationships (including use of subcontractors), develop a risk profile, and incorporate these findings into the overall risk assessment relating to third-party risk management.

Governance and oversight by the board of directors and management will be a focus of the Agencies and should be commensurate with the banking organization's risk appetite and the level of risk and complexity of its third-party relationships. Consideration should be given to the development of a written risk appetite statement. As with all risk-based programs, bank examiners will expect banking organizations to have a risk assessment that addresses their overall third-party risk management processes and incorporates an understanding of each third-party relationship sufficient to develop a third-party relationship risk profile that includes higher risk relationships and those that are designated as critical. Residual risks identified should be brought to the attention of the board of directors and should be consistent with the risk appetite of the banking organization. In addition, the development of a risk appetite statement may also be a useful tool in navigating some of the more challenging residual risks.

The third-party risk management life cycle should be clearly articulated, with an emphasis on due diligence and ongoing monitoring as arguably the most important components. Comprehensive due diligence should be conducted based upon risks identified and collaborative efforts. Reliance on others is reasonable, and the risks or reliance should be identified and managed appropriately. Ongoing monitoring of these relationships should be diligent, with appropriate staffing and expertise, and risk-based training should be provided when necessary. In situations where there is collaboration and reliance on others for certain monitoring activities, these risks must also be considered and accounted for.

Business relationships with third parties engaged in lending, payment, or deposit activities for the benefit of the banking organization or through the banking organization should be evaluated by banking organizations using both the third-party risk management guidance and the various risk management processes and rules that apply to traditional lending and deposit relationships.

Finally, banking organizations are responsible for ensuring that their third-party relationships are in compliance with applicable laws and regulations, including but not limited to those designed to protect consumers (such as fair lending laws and prohibitions against unfair, deceptive, or abusive acts or practices). These areas require specialized expertise, and banking organizations should ensure that appropriate staff are included in these review processes and incorporated into all phases of the third-party risk management life cycle. Consumer protection is a priority of the Agencies, and banking organizations should ensure that sufficient transparency exists within their third-party relationships to ensure legal compliance and that consumer complaints received by third parties are monitored and resolved effectively.

Key Takeaways for FinTech Companies

To develop and maintain relationships with banking organizations, third-party firms need to expect that significant amounts of due diligence and other information may need to be shared with the banking organization during all phases of the third-party relationship life cycle. When relevant and available, a banking organization may request to review system and organizational control (SOC) reports and any conformity assessment or certification by independent third parties related to relevant domestic or international standards. Management information systems, information security, and operational resilience will be a focus, and a third party should maintain accurate inventories of its technology and its contractors to enable banking organizations to understand and assess the third party's information systems and related controls.

The third-party life cycle also references the use, sharing, protection, and storage of banking organization, third-party, and customer data. FinTech companies should be prepared to demonstrate to banking organizations comprehensive systems and internal controls to ensure compliance. The Agencies recently issued final rules on incident response that include specific requirements relating to service companies, and the Consumer Financial Protection Bureau has also been focusing on the security and privacy of customer data and has issued proposed rules in this area.

Banking organizations will be particularly focused on subcontractor relationships and the strength of FinTech companies' controls and oversight concerning subcontractor activities. The Final Guidance does not use the term "critical subcontractors" and lessened some of the due diligence obligations for banking organizations; however, the Final Guidance sets forth clear expectations and requirements on third-party oversight in this area, such as maintaining an inventory of subcontractor relationships, the significance of the activity, and the degree of oversight conducted.

FinTech companies and other firms, including cloud providers, should also be aware that they may be subject to Agency oversight, examination, and enforcement to the extent that the activities provided to the banking organization fall within the BSCA. The BSCA specifically provides authorization for the Agencies to "regulate and examine" a service provider's performance of services to a depository institution, and this authority has been applied by the Agencies only to the extent of the services being provided by the service provider.

The Final Guidance also highlights consumer protection in most of the components of the third-party relationship life cycle. The Agencies will not tolerate any third-party relationships, including BaaS arrangements, that are unfair, deceptive, or result in customer harm, abuse, or unfair access. In this regard, banking organizations may demand transparency into the consumer complaints received by the third party to ensure that customer complaints are handled appropriately and allow the banking organization to take steps to remediate or terminate the relationship, if appropriate.

The Agencies are also focused on Bank Secrecy Act (BSA) and sanctions compliance, and these areas need to be incorporated into any third-party arrangement. The respective obligations of the parties should be clearly articulated in contracts and understood by all parties. Banking organizations may demand verification of these obligations due to the significant risks. A banking organization should never be in a position of having to sort out which party is responsible for BSA and sanctions compliance after the product or service has been launched, and it should have a clearly defined relationship, sufficient visibility, and adequate risk-based controls to ensure that the identity of the ultimate customer is not obscured.

Third-party service providers should understand that banking organizations are required to have a strong culture of compliance that will need to be reflected in FinTech companies that partner with banking organizations. In fact, the Financial Crimes Enforcement Network (FinCEN) has issued guidance concerning how to integrate a

culture of compliance into an organization pertaining to BSA/anti-money laundering (AML) compliance with many of the concepts applicable across other compliance obligations. FinTech companies should take note of this guidance to better understand the significant expectations placed on financial institutions. The companies that ignore or do not instill a culture of compliance on par with the banking industry will be at a competitive disadvantage.

Conclusion

We expect that the Agencies will continue to focus on third-party relationships, BaaS relationships, and other FinTech relationships, as well as related compliance matters (consumer and BSA/OFAC compliance). Some of the questions that remain unanswered include the scope of the additional resources that the Agencies will be providing to smaller and less complex banking organizations and whether reliance on others and collaboration for various components of the third-party life cycle will provide sufficient comfort to banking organizations and the Agencies in administering the many expectations and factors set forth in the third-party relationship life cycle. There are also questions concerning the expanding use of various utilities—including the internet—and cloud services and how these areas will be treated by the Agencies in light of some of the challenges recently described in the Department of the Treasury assessments. Finally, questions related to protections and privacy of data, which are subject to continuing developments and regulations, remain.

Authors

Explore more in

Fintech & Payments Financial Services & Investments