KPMG

Regulatory Alert

Regulatory Insights

July 2024

Regulatory Focus: Third Party, "Nth" Parties, Intermediaries & Service Providers

KPMG Insights:

- ***Growing Regulatory Pressure:*** *Intensifying pressure to manage risks related to the variety of third-party arrangements, in part due to increasing dependencies and interconnections between companies; regulatory focus on safety and soundness, compliance, resiliency, and reputation risks.*
- ***Risk-Based Approach:*** *Requires a risk-based strategy to manage risks throughout the relationship lifecycle, regardless of the relationship type or activities; expectation to rank parties/providers based on "criticality" and risk to the enterprise.*
- ***Third Party Monitoring:*** *Expectation for ongoing monitoring of practices and adherence to company policies, standards, and thresholds (e.g., access, use, security, privacy, retention, deletion, sharing/monetization), particularly related to sensitive systems or data; increased bar for reporting metrics to the Board.*

The growing number and complexity of third-party arrangements (e.g., direct, indirect, "nth" party) is increasing interdependencies within and between companies and industries, elevating risks to companies and their customers across multiple risk areas (e.g., compliance, data management, cybersecurity, fairness, and BSA/AML), and drawing heightened attention from regulators. Recent regulatory actions responding to party/provider risks include:

- Releases from the Federal banking agencies:
  - Prepared remarks from the Acting Comptroller of the Currency entitled "Size, Complexity, and Polarization in Banking."
  - An interagency request for information on "Bank-Fintech Arrangements Involving Banking Products and Services Distributed to Consumers and Businesses."
  - A "Joint Statement on Bank's Arrangements with Third Parties to Deliver Deposit Products and Services."
- BCBS "Draft Principles for the Sound Management of Third-Party Relationships."

Regulators are focusing on risk management and governance across the full third-party risk management (TPRM) lifecycle for all types of party/provider relationships with the expectation that more rigorous oversight will be afforded arrangements related to a company's critical services.

Federal Banking Agency Releases

The Federal banking agencies (together, the Federal Reserve Board (FRB), Federal Deposit Insurance Corporation (FDIC), and Office of the Comptroller of the Currency (OCC)) take the following actions related to the increase in bank-nonbank arrangements:

Acting Comptroller Remarks

The "increasing complexity of bank-nonbank relationships" is one of three long-term trends the Acting Comptroller says are reshaping banking. He outlines how advances in technologies and increased digitalization have given rise to growing numbers of nonbank financial technology firms (fintechs) that, in turn, have resulted in a shift away from direct banking relationships to "long-intermediated chains of discrete services" (e.g., core processors to support operations and functions; cloud service providers to support

digitalization initiatives). The Acting Comptroller adds that the continued evolution and proliferation of bank-nonbank arrangements "has highlighted the need for more granular approaches and greater engagement between the [Federal banking agencies] and nonbank fintechs." He names risks related to deposit arrangements, payments arrangements, and lending arrangements as priority areas.

Interagency Request for Information Re: Fintech Arrangements

The agencies observe that although bank-fintech arrangements can vary significantly in structure and product and service offerings, they commonly fall into one or more categories including deposit taking (e.g., checking and savings accounts), payments (including card issuance and digital wallet capabilities), and lending activities (e.g., unsecured consumer or small business loans). Through the Request for Information (RFI), the agencies describe each of these arrangement structures, the role of intermediate platform providers, and "the risks the agencies have seen manifesting and arising from these arrangements." Broadly, the identified risks include accountability, end user confusion, rapid growth, concentration and liquidity management, and the use and ownership of data and customer information.

Comments will be accepted for a period of 60 days following publication in the Federal Register. Example areas of inquiry include:

- The adequacy of descriptions or categorizations of bank-fintech arrangements.
- Data used to monitor risk, ensure compliance or otherwise manage bank-fintech arrangements.
- Methods for determining whether the end user is a customer of the bank or the fintech or both.
- Variations in the range of practices for maintaining safety and soundness and compliance based on the type of arrangement.
- Effective techniques or strategies in managing the impact of rapid growth.
- The role of intermediate platform providers in amplifying or mitigating risks and influencing operational and compliance issues.
- The range of practices regarding planning for when a fintech company or intermediate platform provider exits an arrangement, faces a stress event, or experiences a significant operational disruption.
- Additional clarifications or further guidance that would be helpful to banks with respect to bank-fintech arrangements.

Joint Statement Re: Deposit Products and Services

The agencies issue a Joint Statement to remind banks of potential risks associated with arrangements between banks and third parties to deliver, directly or indirectly. bank deposit products and services to end users; the Joint Statement also highlights examples of effective risk management practices that banks may want to consider.

Potential risks identified include:

- A lack of direct contracts across multiple layers of third-party and subcontractor relationships challenging the ability to identify, assess, monitor, and control risks.
- Leveraging new technologies or new methods for which staff do not have prior experience or sufficient training.
- Rapid growth, either in number of arrangements or size of arrangements, that outpaces operational capabilities.
- End user confusion related to deposit insurance coverage, and potentially misleading or inaccurate information included in marketing materials or other statements regarding deposit insurance coverage.
- Effective compliance management, including complaint management, error investigation and resolution, and consumer protection-related disclosures.

BCBS Draft Principles

The Basel Committee on Banking Supervision (BCBS) releases draft Principles for the Sound Management of Third-Party Relationships. The BCBS states the draft contains a "new set of principles to reflect the evolution of a larger and more diverse [third-party service provider] environment." Twelve high-level principles provide guidance to banks and prudential supervisors on effective third-party risk management across the full third-party relationship lifecycle, aiming to enhance banks' ability to withstand operational disruptions and mitigate the impact of severe disruptive events that may arise from increasing dependencies on, and interconnectedness with, third parties. Key concepts embedded into all stages of the lifecycle and applicable to all principles include "criticality," "concentration risk," and "proportionality" as well as "intragroup third-party service providers" and "nth parties and supply chains."

Comments on the draft document will be accepted through October 9, 2024. Once finalized, the principles will supersede the Joint Forum paper, "Outsourcing in Financial Services", released in 2005.

Key areas of regulatory focus across risk management, the lifecycle for party/provider relationships, and governance practices include those highlighted in the table below.

Area of Focus	Description
Risk Management	Established and formalized: — Risk-based approach to management programs for all third-party relationships, tailored to the company's size, complexity, and risk profile as well as to the nature of each relationship (including relevant laws and regulations) — Inventory of all third-party relationships (by contract or otherwise) — Risk assessment of each third-party relationship, with periodic updates and documentation of changes made based on changes to each third-party's risk profile — Requirement for more comprehensive and rigorous oversight and risk management of parties/providers that support "higher-risk" or "critical activities" (as defined and identified by the company) — Metrics to assess effectiveness of the TPRM program — Strategic plan for resources, infrastructure, technology controls, and organizational capabilities to manage risks. — Ongoing monitoring of the services delivered to make sure that service level agreements are met, changes to services are updated on both sides in a timely manner and that accurate billing per contract can be monitored. — Board oversight of the TPRM program. — Contingency plans to terminating a relationship in a timely and effective manner and replacing third-party as needed.
Lifecycle	Effective TPRM practices that follow the lifecycle of third-party relationships and involve knowledgeable and skilled staff at each stage and across disciplines, as appropriate (e.g., compliance, risk, technology, legal), including: — **Planning:** Evaluation and consideration of risk management needs before entering a third-party relationship. Key issues may include: the third party's access to or use of customer information and/or access to the company's systems; the company's ability to adequately oversee the business arrangement; contingency plans to transition away from the third party. Certain third parties (i.e., those supporting "higher-risk" or "critical activities") may warrant a greater degree of planning and consideration, such as board approval. The integration of the various source to pay and contract life cycle management steps with the TPRM program is key to avoid silos. — **Due Diligence and Selection:** – Evaluation of capability to appropriately identify, monitor, and control risks associated with a particular third-party relationship (scope and degree of due diligence should be commensurate with the level of risk and complexity of the third-party relationship). Areas considered include the third party's: • Legal/regulatory compliance (e.g., licenses and ability to comply with US Federal and State Laws in place around products and services); human resources (e.g., staffing, experience, culture); operational resilience and cybersecurity practices; reliance on subcontractors and/or contractual arrangements with other parties. – Documentation of any limitations on due diligence efforts and consideration of alternatives to mitigate related risks. (Note: Banking organizations may use external parties, such as consultants or consortiums, to supplement the information gathering.)

	— **Contract Negotiation:** – Tailoring the level of detail and comprehensiveness of contract provisions based on the risk and complexity posed by a particular relationship. Key terms may include: • The company's rights to audit, monitor compliance, and require remediation; responsibility of both parties to comply with applicable laws and regulations; notification requirements (e.g., data incidents, exception reports, strategic/organizational changes); reporting requirements; data access, use, and ownership. – Conducting periodic reviews of executed contracts to ensure provisions continue to address pertinent risk controls and legal protections; renegotiation of contracts in response to changing risk assessments or laws and regulations. — **Ongoing Monitoring:** – Confirmation of the quality and sustainability of a third-party's practices and controls, escalation of significant issues or concerns, and appropriate response when identified. – Evaluation of the effectiveness of the third-party relationship, including whether it continues to align with the company's strategic goals, business objectives, risk appetite. – Periodic (or more frequent, where appropriate) monitoring for third-party relationships that support "higher risk" activities, including "critical activities". — **Termination:** Assessing and executing termination of a third-party relationship, giving consideration to appropriate risk management of data retention and destruction, information system connection and access controls, and customer impacts.
Governance	Governance practices that facilitate sound and effective TPRM, including: — Oversight and accountability, including delineation of Board and management roles, responsibilities, performance metrics, and standards, Board approval of the TPRM program, risk appetites, and disruption tolerances, and Board participation in selection, approval, and monitoring of third-party relationships and related data and systems integrity, corporate governance, strategic planning, liquidity and funds management, interest rate risk, earnings, and asset growth. — Periodic, independent reviews (audits) of the TPRM program. — Robust documentation and clear reporting channels, both within the company and to/from third parties, that facilitate Board and management oversight, accountability, monitoring, and risk management of third-party relationships and performance.

For more information, please contact Amy Matsuo or Greg Matthews.

Contact the author:

Amy Matsuo
Principal and National Leader
Regulatory Insights
amatsuo@kpmg.com