Heightened Supervision & Enforcement Trends

What it Means for Banks and Non-Bank Third-Party Service Providers

Andrew Bigart
Partner | 202.344.4323 | abigart@venable.com

Max Bonici
Counsel | 202.344.4832 | mbonici@venable.com

VENABLE LLP

Agenda

1. Overview of bank supervision and enforcement powers
    - General
    - Third-Party Service Providers
2. Supervisory environment since the Spring 2023 bank failures
3. Recent trends in enforcement actions
4. Implications for bank / service provider relationships and contracts

VENABLE LLP

Overview of bank supervision and enforcement powers

Federal Banking Agencies

VENABLE LLP

Safety and Soundness

- Banks are subject to a significant degree of regulation because of their unique role and powers
- To assess compliance with applicable statutes and regulations, the federal banking agencies ("FBAs") conduct supervision, including on-site examinations and issue critical findings
- Main statutory authority for supervision is the Federal Deposit Insurance Act ("FDIA")
  - 12 USC 1831p–1 covers the standards for safety and soundness
  - 12 USC 1820(d) covers annual on-site examinations for all insured depository institutions
    (e.g., national banks, state-chartered banks, federal or state-chartered thrifts)
- Safety and soundness is a key lens through which the FBAs consider what a bank does and how it does it

VENABLE LLP

Which activities are subject to supervision?

Overall safety and soundness of the bank

- Capital and liquidity, assets and earnings
- Credit underwriting, lending concentration, other market risks
- Board and management functions/roles and requirements

Compliance supervision

- Consumer and related-issues are important
  - Fair lending and fair credit laws
  - Disclosure requirements, data privacy, and unfair, deceptive, or abusive acts or practices
  - Community Reinvestment Act (which has its own evaluation process and ratings)
- As well as certain specialized exams for particularly important or complex issues:
  - Bank Secrecy Act ("BSA") / anti-money laundering ("AML") and other anti-financial crimes obligations, including economic sanctions
  - IT and data systems, including cybersecurity and data privacy

VENABLE LLP

Supervision covers how banks may engage in activities

Modern bank operations use a range of third-party service providers ("TPSPs")

Most banks do not perform all major operations in-house, especially as compliance costs increase and specialization continues

- Banks use TPSPs for major and relatively minor operations or needs (e.g., from technology solutions to cleaning crews)
- Bank staff relies on information or processes from TPSPs and often coordinates and manages activities that TPSPs perform

- Technology and data service providers are particularly important
  - IT service providers run bank systems, process lending models, provide AI solutions, and more
  - Smaller banks are particularly dependent on core ledger and other IT providers
  - Large banks also face significant risks when they outsource these activities
- Understanding and controlling for third-party risk is important, but bringing operations in-house doesn't mitigate all risk

VENABLE LLP

Supervision covers bank sponsorships / partnerships

In addition to using service providers, many banks sponsor or contract third parties (fintechs) to help provide financial services directly to customers, primarily in areas involving:

- Marketing or processing of cards, ACH, and other payment services
- Issuing prepaid or credit cards
- Consumer or commercial lending
- Banking-as-a-Service

All fintechs typically need a bank partner in some way:

- Receive, hold, and transfer program funds
- Minimize regulatory licensing and other risks for the fintech (e.g., money transmission, lending, etc.)
- Ensure compliance with payment network requirements

These relationships, however, may present greater risk in certain respects because of the direct customer engagement and role of the fintech in providing the financial services

VENABLE LLP

Agency actions: Pre-enforcement tools

Supervisory rating system (CAMELS, and others)

- The FBAs use these ratings and examination reports to convey whether a bank is in compliance with safety and soundness and other supervisory requirements
  - **C**apital adequacy
  - **A**sset quality
  - **M**anagement (Third-party oversight deficiencies most often show up in the **M**anagement rating)
  - **E**arnings
  - **L**iquidity
  - **S**ensitivity to market risk
- Banks are rated on each component, and a composite rating is also given:
  - 1 — “strong”
  - 2 — “satisfactory”
  - 3 — “less than satisfactory”
  - 4 — “deficient”
  - 5 — “critically deficient”

VENABLE LLP

Agency actions: Informal v. Formal Actions

Informal actions

- Generally appropriate for composite rating of "3" for safety and soundness / consumer compliance
- May also be appropriate when specialty examination areas are rated "3" or when significant weaknesses are identified in BSA/AML compliance
- An FBA may also pursue an informal enforcement action against a higher rated institution, if the specific facts and circumstances make such an action appropriate

Formal actions

- Formal action is generally initiated against an institution with a composite rating of "4" or "5" for safety and soundness, or for consumer compliance if there is evidence of unsafe or unsound practices and/or conditions or concern over a high volume or severity of violations
- Specific facts and circumstances may warrant the pursuit of a formal action, even if an institution has a composite rating of "3" or higher for safety and soundness or for consumer compliance
  - For example, certain actions, such as CMPs and restitution, may be taken based upon actionable misconduct that may be unrelated to the institution's supervisory ratings or condition
- When formal action is considered but ultimately not pursued (e.g., when a CMP matrix score suggests no CMP be assessed) the FBA may send a supervisory letter

VENABLE LLP

Agency actions: Pre-enforcement tools

Matters requiring attention ("MRAs")

- When identified in an exam report, these must be addressed in a "reasonable" period
- MRAs are generally thought of as potential risks to safety and soundness, and they will remain open until examiners determine the bank has taken appropriate corrective action

Matters requiring immediate attention ("MRIAs")

- Matters of significant importance and urgency that the bank must address immediately
- These pose significant risk to the safety and soundness or represent significant noncompliance with applicable laws or regulations
- MRIAs can also result from repeat criticisms for which the bank has taken insufficient attention or from matters with the potential to cause significant consumer harm

VENABLE LLP

Agency actions: Pre-enforcement tools

Bank Board Resolutions ("BBRs")

- Informal commitments adopted by an institution's board of directors (often at the request of the FBA) directing the institution's personnel to take corrective action regarding specific noted deficiencies

Memorandums of Understanding ("MOUs")

- MOUs may be used instead of BBRs when there is reason to believe the deficiencies noted during an examination need a more structured program or specific terms to effect corrective action.
- An MOU is an informal agreement between an institution and the FBA, signed by both parties. A state authority may also be a party (as applicable)
- MOUs are designed to address and correct identified weaknesses in an institution's condition, or violations or unsafe or unsound practices at the institution
- Use of a MOU does not prevent the FBA from subsequently pursuing formal enforcement action if such formal action is required by law or if the FBA believes the institution's management is unwilling or unable to voluntarily take necessary corrective action

Agency actions: Enforcement tools

FBAs are authorized by statute to initiate civil enforcement actions

- Primarily based on 12 USC 1818, part of the FDIA, but there are other sources of authority

Cease and desist orders ("C&Ds") and written agreements

- These orders are issued when the FBA determines a bank has engaged (or is about to) in unsafe or unsound practices or has violated (or is about to) a law or regulation
- C&D orders flow from the supervisory process where violations are identified, and often are voluntarily entered into by the banks as part of a written agreement

Civil money penalties ("CMP")

- There are three tiers of potential CMPs based on the severity of the violation
- CMPs are not required in connection with a C&D, but for certain violations, such as when BSA/AML is involved, CMPs are common

Certain individuals that are institution-affiliated parties ("IAPs") may be subject to individual liability

- CMPs can be applied against both the institution and IAPs
- Individuals may also be removed/suspended/prohibited from working in the banking industry

VENABLE LLP

Supervisory environment

Since the Spring 2023 bank failures

VENABLE LLP

Supervision

We are currently in a regulatory supercycle following the 2023 regional bank failures

- Safety and soundness is the focus
- Agencies are looking at **balance sheet basics** and fundamental risk management practices, including in enforcement actions
- **Third-Party Risk Management** issues pervade
- Expect examiners to use a fine-tooth comb in all areas of bank businesses and structures
- Supervisory rating downgrades are possible, or higher ratings may be harder to get
- Non-banks are not immune from the regulatory uptick due to ripple effects and focus on interconnections between banks and non-banks
- In recent remarks, the acting Comptroller has floated more specific **operational resilience** and risk requirements for large banks and their third-party service providers

VENABLE LLP

Increased regulation and rulemaking activity

Increased supervisory scrutiny

Increased enforcement activity and specificity

Less tailoring

Less time (to regulate; to respond)

Supervisory trends

Response to the 2023 bank failures

- Although not directly related to third parties, the failures have focused public and Congressional scrutiny on how the FBAs conduct supervision
- In April 2023, the Federal Reserve released a review of its own supervisory short comings with respect to Silicon Valley Bank (SVB)
  - Fed said its supervisors had failed to fully grasp how vulnerable the bank actually was and hadn't pushed hard enough to make sure the bank promptly fixed the problems they did spot.
  - The FDIC released a similar review of its supervision of Signature Bank

Increased focus on governance and board oversight

- Highlighted as one of the causes of SVB's rapid growth and ultimate failure
- FDIC proposed new governance guidelines for FDIC-regulated banks over $10B

Fintech partnerships have come under increased scrutiny

- Proliferation of partnerships, deposits at small banks, and BSA/AML concerns
- Federal Reserve created the Novel Activities Supervision Program, which focuses on four categories, including "complex, technology-driven partnerships with non-banks"

VENABLE LLP

Supervision Update—Public Statements

The Fed's Vice Chair for Supervision recent explained that the Fed has increased supervision and will continue to do so

- "For large and more complex regional banking organizations, including firms that are growing rapidly, we are assessing such a firm's condition, strategy, and risk management **more frequently**, **and deepening** our supervisory interactions with the firm"
- Supervisors have increased their scrutiny of any high volumes of **unrealized losses** at financial institutions
  - "For a small number of banks with a risk profile that could result in funding pressures for the firm, supervisors are **continuously monitoring** these firms"

The Fed's Chair, Jerome Powell, also recently testified before Congress that the Fed is working on developing a "new rulebook" for more robust examinations

- "If you look at Silicon Valley Bank, we weren't quick enough and we weren't effective enough…[s]o we're working hard to develop a new rulebook and another set of practices"
- It is "still going to be evidence-based and fair, but it's going to involve **earlier interventions and more effective ones**"

VENABLE LLP

Recent GAO Findings—"More Timely Escalation"

A recent U.S. Government Accountability Office recommends that the Fed and FDIC should make policy changes to give examiners less discretion when dealing with banks

GAO concluded that the Fed's examination policies

- "Often are not clear and specific" about when a supervisory concern should be escalated from a warning to a more serious informal or formal enforcement action
- "Often do not include measurable criteria that act as a trigger to prompt action for addressing deficiencies"
- GAO noted that the FDIC has already updated its examiner policies

GAO recommends

- "Establishing clear, specific procedures with measurable criteria could help clarify when escalation to informal or formal enforcement action would be required and help ensure that regulators take earlier and more forceful actions to compel bank management to correct deficiencies"
- (A longstanding recommendation:) Expand the FBA's **prompt corrective action framework** by adding "**triggers" based on factors other than capital levels**

VENABLE LLP

Recent trends in enforcement actions

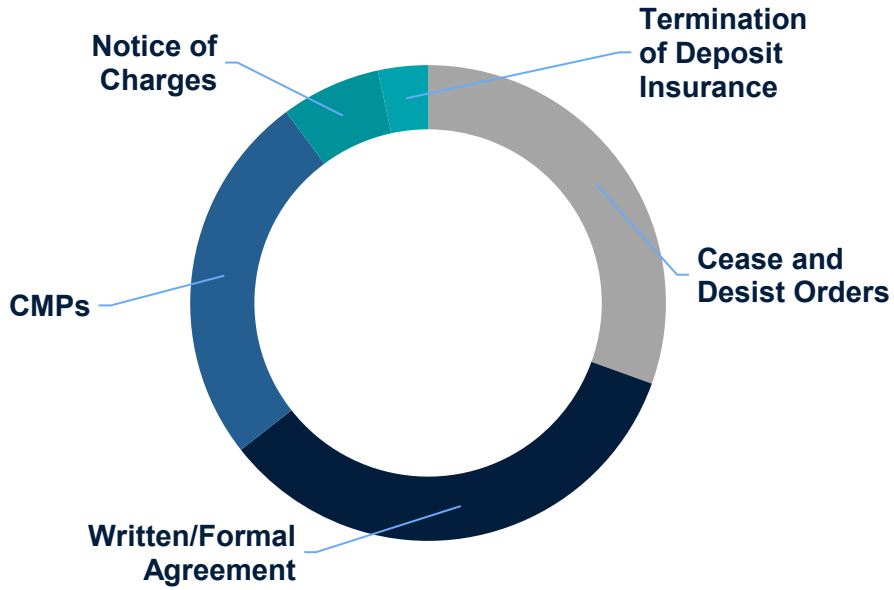
Federal Banking Agencies

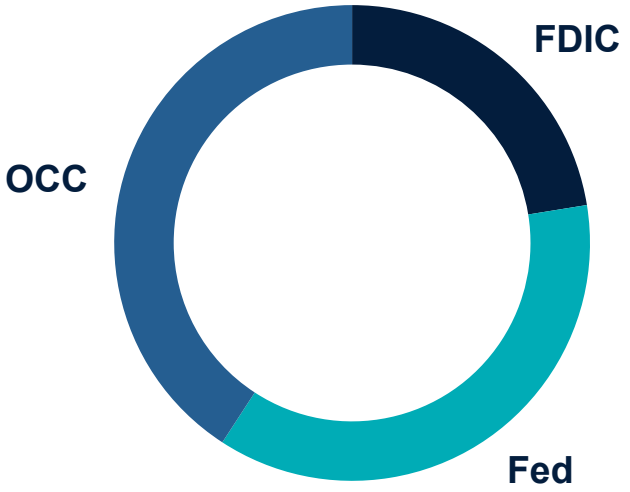
VENABLE LLP

Enforcement trends
April 2023 to March 2024

50 Enforcement actions

4 Average enforcement actions per month





Venable LLP research based on public enforcement actions by federal banking agencies, with certain exclusions (e.g., actions against individuals).

VENABLE LLP

Enforcement developments

- Consumer protection (e.g., UDAP/UDAAP), fair lending, and BSA/AML issues remain important enforcement priorities for which CMPs are expected to be assessed
- We are also seeing kitchen-sink enforcement actions that cover everything a bank is expected to do—at a granular level—in C&D orders
  - Board responsibilities
  - Policies and procedures
  - Capital plans
  - Liquidity management
  - Concentration risks
  - Credit review/analysis/losses
  - Data management
  - IT and systems
  - Internal audit
  - Internal controls

> unsafe or unsound practice(s), including those relating to oversight by its management and board of directors ("board"); strategic planning; capital planning; stress testing; policy development and approval; management and board reporting; contingency funding planning; model risk management; concentration risk management; credit review; credit analysis; risk assessment; allowance for credit losses methodology; data management; internal audit; and internal controls. These unsafe or unsound practice(s) are included in, but may not be limited to, the areas of corporate governance and enterprise risk management, credit underwriting and administration, liquidity risk management, and interest rate risk management;

VENABLE LLP

Enforcement related to third-parties

25% of recent enforcement actions mention third-party risk management deficiencies and affirmative steps to bolster compliance

- Banks are expected to manage their **non-bank vendors** in line with the Guidance
- Issues involving banks' management and oversight of **non-bank affiliates** have also been the subject of recent enforcement actions

(a) the process for how the Bank selects, assesses, and oversees third parties;

(b) the process for the identification and classification of all vendors based on risk criteria and risk assessment;

(c) written contracts that outline the rights and responsibilities of all parties;

(d) vendor review cycles that are based on the degree of risk posed by each vendor;

(e) roles and responsibilities of management relating to due diligence and ongoing monitoring of third parties; and

(f) documentation and reporting that facilitates Board and management oversight, accountability, monitoring, and risk management associated with third-party relationships; and

VENABLE LLP

Small Business Bank (Kansas)

- Bank specializing in serving small businesses, solopreneurs, and freelancers, offering checking, high-yield savings accounts, and business debit cards hit with a C&D Order.
- It doesn't have any subsidiaries or affiliates, other than its parent bank holding company (BHC). It has $100 million in total assets—**0.1% the size of a "large bank"**
- Nearly 20-page action rattles off a laundry list of safety and soundness and good governance considerations applicable to all banks, instead of merely focusing on BSA/AML (though those issues are included too) and consumer-facing compliance issues, including:
  - interest rate risk management
  - liquidity and funds management
  - diversification of sources of funding
  - enhanced liquidity stress test scenarios
  - periodic independent reviews/evaluations of the entirety of the liquidity risk management process
  - sufficient staffing and training, risk limits and appropriate metrics, as well as board governance
  - that BHC serve as a source of strength for the bank

VENABLE LLP

Blue Ridge Bank, N.A.

January 2024 consent order

- The OCC found the bank to be in "troubled condition" after alleged continuous failure to address BSA/AML compliance issues
- Among other remediation steps, the bank must develop a better risk-based program to ensure that the bank and accounts related to third-party fintechs meet BSA/AML compliance requirements, including those related to filing SARs
- As in other TPRM-related enforcement actions, the OCC expressly incorporates by reference and reviews in detail the components of the TPRM Guidance
- The OCC also pointed to OCC-specific guidance, in this case, an OCC guide for community banks conducting due diligence on fintechs (OCC Bulletin 2021-40)

Builds on a previous enforcement issues

- 2022 written agreement targeted similar issues
- The bank had announced in November 2023 that it would reduce its nearly 50 BaaS partnerships to only a "limited number" with "a commercial focus or strong consumer traction"

VENABLE LLP

Lineage Bank

The FDIC recently released a January 2024 consent order involving Lineage Bank that would require it to implement a strategic overhaul overseen by its board of directors, increase its risk controls and capital and offboard some of its fintech partners

Notable features include (among others):

- Clear focus on **FBO accounts and ACH-related products and services**
- TPRM-related requirements are imposed on **all fintechs** with which the bank has relationship—both third-party fintechs and fintechs with which the bank has a direct relationship
- Bank must retain a third-party to review its TPRM program and conduct the due diligence expected under the TPRM Guidance
- Bank must limit annual growth of assets and liabilities to under 10%, terminate "significant" fintech partnerships and increase its Tier 1 regulatory capital
- Order subjects much of TPRM program, including onboarding for new fintech partners, to the review and comment of the FDIC Regional Director for the bank

VENABLE LLP

Enforcement Risks for Third Parties

In addition to direct enforcement against a bank, federal and state regulators may bring actions against the bank's service provider or third party partner, which can create reputational, financial, and operational risks for the bank.

In particular, federal regulators have been aggressive in bringing enforcement actions against providers of payment processing and related services.

- The Consumer Financial Protection Bureau has flagged processing payments for companies engaged in fraudulent activities as a UDAAP.
- The Federal Trade Commission has brought numerous enforcement actions against payment processors, payment facilitators, and other payments companies.

VENABLE LLP

FTC and CFPB Actions against Payment Companies

Theories of Liability

- The processor intentionally facilitated fraud
- In the face of obvious red flags, the processor ***turned a blind eye*** to fraud
- The processor provided substantial assistance to a person that violated consumer protection rules
- The processor is jointly and severally liability with the merchant for the full volume of sales processed

Remedies Sought

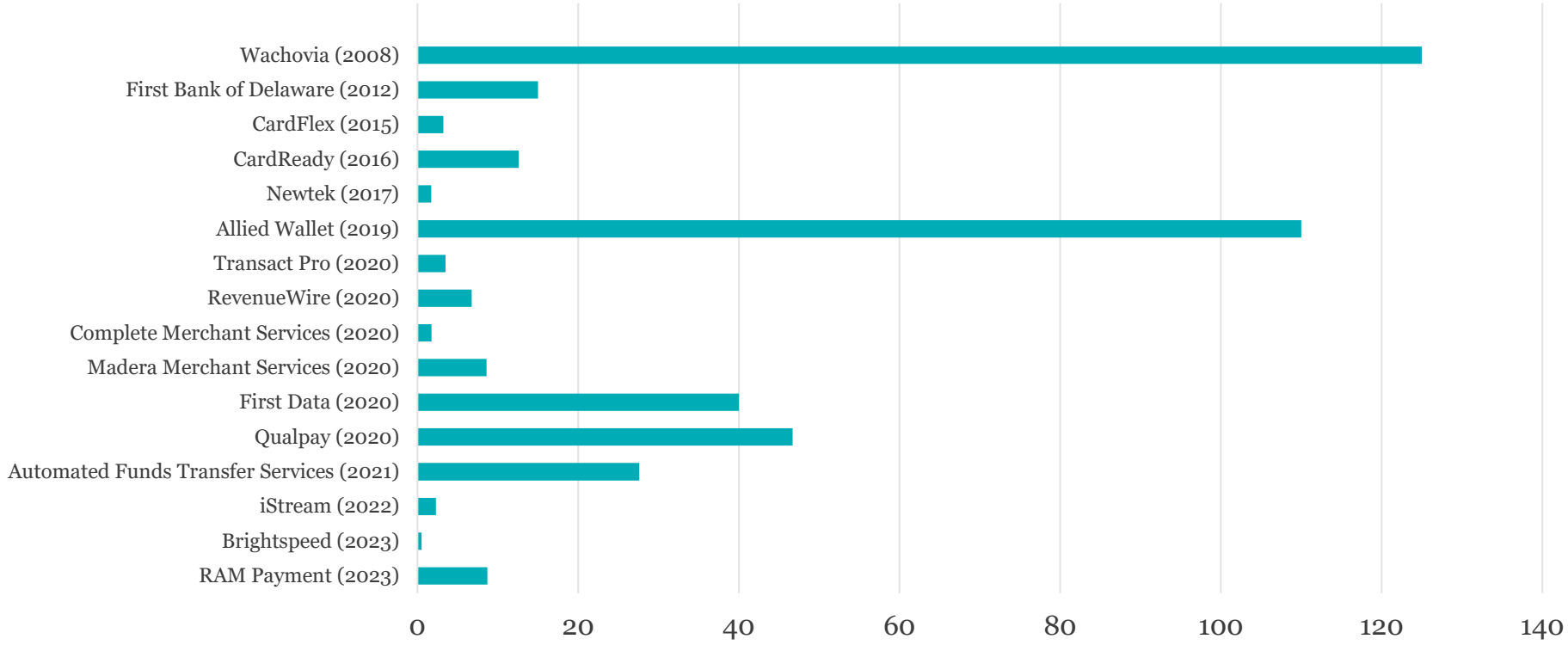
- Injunctive relief
- Rescission of contracts
- Disgorgement of ill-gotten gains
- Redress to consumers
- Liability for individuals (company officers, directors, managers) (sometimes)

Common Settlement Terms

- Ban on operating as a processor (extreme cases)
- Ban on servicing certain industries or merchants using certain sales practices
- Merchant screening and monitoring requirements more restrictive than industry standard
- Payment of a monetary penalty
- Sales agent onboarding and monitoring requirements
- Notices to bank, ISO, and other partners
- Ongoing government oversight and compliance reporting

VENABLE LLP

Monetary Penalty ($ Millions)



VENABLE LLP

Bank / Service Provider Relationships

Managing Risks

VENABLE LLP

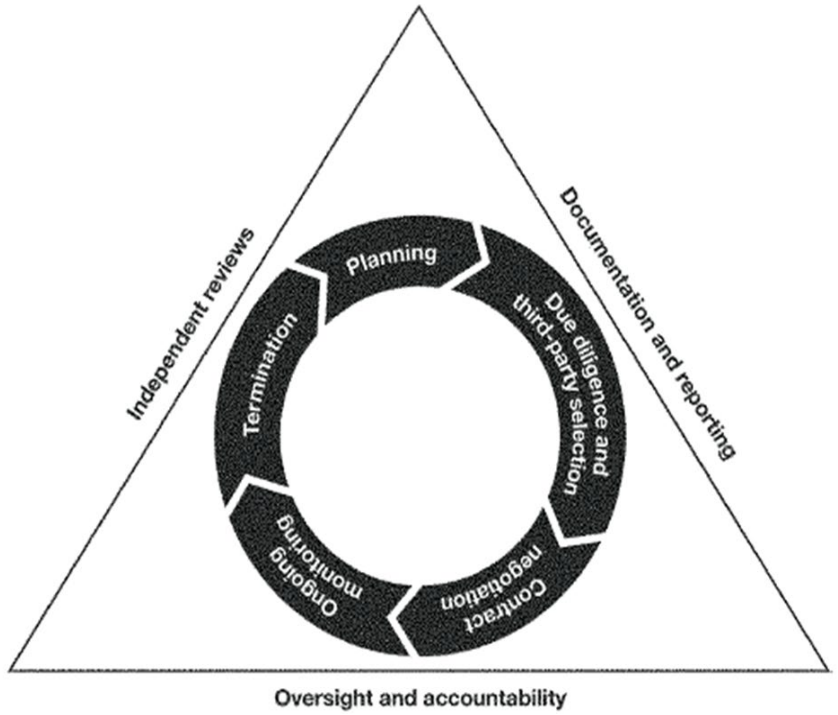
Third-party relationships in focus

The FBAs finalized interagency guidance ("Guidance") in June 2023 (88 FR 37920)

- Provides a harmonized view of safe and sound risk management for all stages of the life cycle of third-party relationships
- Builds on previous separate guidance regarding third-party risk management: FDIC (2008), Federal Reserve (2013), and OCC (2013, 2020), using much of the OCC framework
- Emphasizes that the use of third parties does not diminish a bank's obligation to ensure safe and sound practices "to the same extent as if its activities were performed by the banking organization in-house"

VENABLE LLP

Third-party relationship life cycle



- The Guidance identifies five stages of a third-party relationship's life cycle:
  1. Planning
  2. Due Diligence & Third-Party Selection
  3. Contract Negotiations
  4. Ongoing Monitoring
  5. Termination
     (Note: Termination is not hypothetical)

- The FBAs outline their expectations for the factors banks should consider in each stage and ways to mitigate potential risks
- The Guidance provides significant detail for the Due Diligence & Third-Party Selection and Contract Negotiations stages
- But recent events indicate that Ongoing Monitoring may involve the most risk/supervisory and enforcement attention

VENABLE LLP

Guidance: Tailoring practices for risk management

The FBAs recognize that risk varies among different third-party relationships

- A bank should "analyze[] the risks associated with each third-party relationship and tailor[] risk management practices, commensurate with the [bank's] size, complexity, and risk profile and with the nature of the third-party relationship"
- Critical activities should be subject to stronger oversight and management, and these activities include those that:
  - Cause a bank to face significant risk if the third party fails to meet expectations
  - Have significant customer impacts
  - Have a significant impact on a bank's financial condition or operations

To conduct effective ongoing risk management, a bank should be:

- "[m]aintaining a complete inventory of its third-party relationships and periodically conducting risk assessments for each third-party relationship"

VENABLE LLP

Guidance: Effective practices and governance

- Oversight and accountability
  - A bank's board of directors is responsible for setting risk appetite, overseeing the third-party risk management processes, and holding management accountable
  - Management is responsible for developing and implementing policies, procedures, and practices commensurate with the risk appetite and its third-party relationships
- Independent reviews
  - A bank should conduct periodic independent reviews of its own process
  - As needed, adjustments to the third-party risk management process should be made and there should be escalation to the bank's board
- Documentation and reporting
  - Documentation and reporting should cover all stages of the life cycle

Third-party relationships and enforcement

The Guidance itself does not contain enforcement mechanisms

- Reviews of third-party risk management programs are incorporated into regulatory supervisory processes
- Examiners will, as appropriate, assess the effectiveness of a bank's program and highlight and discuss "material risk and deficiencies identified" to incorporate third-party relationship considerations into a bank's supervisory rating

As with other issues surfaced in the supervisory process, third-party risk management deficiencies can lead to enforcement actions

- "The agencies may pursue corrective measures, including enforcement actions, when necessary to address violations of laws and regulations or unsafe or unsound banking practices by the banking organization *or its third party*."
- This includes service relationships with affiliates, which "may have different characteristics and risks . . . [but] may not always present lower risks."

VENABLE LLP

The Bank Service Company Act

- The BSCA addresses companies that provide services, such as check and deposit sorting and posting, preparation and mailing of checks and statements, and clerical services
- But section 7(c) is an amendment to the original statute that the regulators have construed more broadly to affect a potentially broad range of activities
- The BSCA could provide an additional means for rather intrusive bank-like scrutiny for non-banks by the FBAs

"**whenever** a [bank] … causes to be performed for itself, **by contract or otherwise**, **any services** authorized under this chapter … such performance shall be subject to **regulation and examination** … **to the same extent** as if such services were being performed by the depository institution itself on its own premises." 12 USC 1867(c).

VENABLE LLP

Improving controls on third-party vendors

Banks might consider comparing their current approach to third-party vendors to comply with third-party risk management expectations and heightened supervisory scrutiny

- Inventory exiting agreements (if not already done)
- Review existing agreements to ensure there is sufficient room for added oversight and accountability
- Renegotiating contracts as needed, or developing a schedule to do so
- Particular emphasis on risk management-related provisions, such as reporting, responding to requests for information, auditing, and consent requirements

Review policies and procedures for conducting initial due diligence and ongoing due diligence on third-party vendors

- Compare processes to the factors listed in the Guidance
- Review policies, procedures, and practices for internal reporting, independent auditing of third-party vendor programs, and board oversight

VENABLE LLP

Practical tips when negotiating contracts

Banks should develop policies and procedures for their TPRM efforts, that cover all stages

- Including negotiating contracts

Clearly divide responsibilities and identification of specific services involved in the relationship

- In fintech partnerships, it may be difficult to determine when the bank is providing services to the third party as its customer and when the third party is providing services to the bank as its service provider
  - The third party is both a customer and a service provider, which not only has an impact on vendor management, but also BSA/AML obligations, data privacy and security, and other compliance requirements

Consider formulating a schedule that distinguishes each facet of the proposed relationship, describes the exact service, and identifies which party is the provider and customer for that service

- While this can be time intensive—and sometimes raises disagreements—the effort will simplify the onboarding, due diligence, and oversight processes in the future

VENABLE LLP

Managing Higher Risk Relationships – Spotlight on BaaS

In recent years banks and fintechs have partnered to offer deposit accounts and other traditional banking products to consumers and small businesses. These partnerships, referred to as “Banking-as-a-Service” (“BaaS”), often include a credit or payments component as well.

- The benefit of BaaS is that it is designed to exempt the fintech from certain state usury, money transmission, and other regulatory and licensing requirements, while also permitting the fintech to focus on customer acquisition, user experience, and technology-assisted transactions.
- The tradeoff for the fintech comes in the form of the bank partner requiring the fintech to comply with various compliance and risk management practices.

BaaS allow consumers broader access to financial services, and involve the use of APIs that connect banks with third party providers of financial services.

VENABLE LLP

Managing Higher Risk Relationships – Spotlight on BaaS

Agreement with fintech should designates responsibilities for important risk management functions:

- Bank Credit / Risk Management Policy – covers prohibited merchants, restricted merchants, underwriting, monitoring and compliance obligations of fintech
- Customer onboarding and agreement requirements for fintech to follow (and approval requirements, depending on the circumstances)
- Contract flow down requirements
- Bank monitoring functions; Fintech exception reporting
- Regulatory Compliance
  - Consumer protection (disclosures)
  - Privacy
  - BSA/AML, etc.
- Audits and reports

VENABLE LLP

Managing Higher Risk Relationships – FBO Accounts

Any payments company or fintech that receives funds as an intermediary between a sender and recipient has potential money transmission licensing requirements.

Common trend among fintechs for managing these risks is to partner with banks that offer custodial accounts opened for the benefit of (FBO) the fintech's customers. In these arrangements, funds flow through an account owned and controlled by the bank and not the fintech.

- Fintech either issues payment instructions to the bank to pull funds from a bank-owned settlement account or instructs its customer to deposit funds into the FBO account.
- Once the funds are received, the bank holds the payments until it receives instructions from the fintech to release them to the designated payee's bank account.
- The funds held in the account are "for the benefit" of the fintech's client(s), indicating that the funds in the account are owed to those parties (and are not owned by the fintech).
- The bank is the only entity responsible for moving the funds, and all funds at rest are in the custody and control of the bank.

Managing Higher Risk Relationships – FBO Accounts

Considerations for Banks

- Who are the fintech's end-user clients (payees) that ultimately receive the funds?
- Can the bank effectively and comfortably monitor transactions and mitigate financial fraud?
- Does the relationship between the bank and fintech address key regulatory requirements (AML, sanctions, etc.)?

The FBO model is often reliant on the fintech's ledgering and reconciliation processes.

- Does the fintech have a reliable ledgering system to ensure management and distribution of funds?
- Small errors may result in large headaches.
- May be particularly complex in a banking-as-a-service ("BaaS") arrangement, where the BaaS provider opens one FBO account for the benefit of multiple fintechs, each with its own portfolio of end-user clients
- Is the bank sufficiently aware of the risks posed by their fintech relationships? Is the bank adequately monitoring and responding to those risks?
- Has the bank discussed its fintech sponsorship program with its regulators, including the use of the FBO model?

VENABLE LLP

Managing Higher Risk Relationships – AI Technology

AI is being implemented in many ways including for AML monitoring, identity verification, underwriting, compliance management, customer service, and cybersecurity.

FIs need to make sure that they understand how the technology works and that any implementation of new AI-based technology improves existing functionalities.

- Review and understand the nature of the technology,
- Develop a plan for how it will be used,
- Implement the technology in accordance with the plan,
- Measure and monitor the technology's performance for potential risks, and
- Make adjustments to the use of technology to address any failings or issues that are identified.

VENABLE LLP

VENABLE LLP