Online Lenders Alliance

Managing Compliance as a Bank Third Party Vendor

Mehul Madia, Sheppard, Mullin, Richter & Hampton, LLP

Max Bonici, Venable LLP

COMPLIANCE UNIVERSITY

COMPLIANCE UNIVERSITY

OLA Online Lenders Alliance

Agenda

- Current Supervisory Environment
- Recent Enforcement Trends
- Interagency Guidance on Third-Party Relationships: Risk Management
- Practical Tips for Third-Party Service Providers
- Drafting Considerations
- Compliance Challenges with Artificial Intelligence

Current Supervisory Environment

- 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.
  - 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

COMPLIANCE UNIVERSITY

Online Lenders Alliance

Increased regulation and rulemaking activity

Increased supervisory scrutiny

Increased enforcement activity and specificity

Less tailoring

Less time (to regulate and respond)

Response to the 2023 bank failures

- Although not directly related to third parties, the failures have focused public and Congressional scrutiny on how the federal banking agencies conduct supervision.
- In April 2023, the Federal Reserve released a review of its own supervisory shortcomings 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.

COMPLIANCE UNIVERSITY

OLA Online Lenders Alliance

Increased Scrutiny for Fintech Partnerships

- According to the Klaros Group, 35% of regulatory actions brought by the FDIC, Federal Reserve, and OCC in Q1 2024 were against fintech partner banks.
  - Q1 2023 it was 10%.
- The focus is on Banking-as-a-Service platforms.
- Proliferation of partnerships, deposits at small banks, and BSA/AML concerns.
- Regulators still playing catch up.
- Federal Reserve created the Novel Activities Supervision Program, which focuses on four categories, including “complex, technology-driven partnerships with non-banks.”

FDIC Spring 2024 Consumer Compliance Supervisory Highlights

- FDIC observed a number of “deficiencies” in bank oversight of third-party relationships.
- Examples:
  - Allowing a third-party partner managing Regulation E error disputes on behalf of the bank to fail to investigate errors alleged with certain online debit card transactions.
  - Failing to give a bank access to all variables used in the credit pricing and underwriting models utilized by a third-party partner in a bank’s loan program.
  - Failing to give a bank an opportunity to review or approve material changes to the underwriting model criteria.

Recent Enforcement Trends

- April 2023 to July 2024: 115 enforcement actions, with an average of 7–8 per month.
- Consumer protection (e.g., UDAP/UDAAP, fair lending, Reg. E error dispute resolution) and BSA/AML issues remain important enforcement priorities.
- Among other remedial actions, enforcement actions have placed limits on a bank's ability to modify existing programs, offer new products, or enter into new third-party relationships without the written approval of the regulator.
- One thing is clear—Banks are expected to manage their non-bank third party relationships.

COMPLIANCE UNIVERSITY

Online Lenders Alliance

Recent Enforcement Trends

The following (non-exhaustive) list of enforcement actions:

- Blue Ridge Bank (two consent orders) No. AA-NE-2022-43, AA-ENF-2023-68 (OCC)
- CBW Bank, No. FDIC-20-0122b (FDIC)
- Metropolitan Commercial Bank, No. 23-018-B-SM 23-018-CMP-SM (Fed)
- Evolve Bank & Trust, No. 22-016-CMP-SM (Fed)
- Cross River Bank, No. FDIC-22-0040b (FDIC)
- Choice Financial Group, No. FDIC-23-0086b (FDIC)
- First Fed Bank, No. FDIC-23-0026b (FDIC)
- First & Peoples Bank and Trust Company, No. FDIC-23-0090b (FDIC)
- Lineage Bank, No. FDIC-23-0041b (FDIC)

Recent Enforcement Trends

- 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.
- The CFPB has flagged processing payments for companies engaged in fraudulent activities, UDAAPs.
- The FTC has brought numerous enforcement actions against payment processors, payment facilitators, and other payments companies

COMPLIANCE UNIVERSITY

OLA Online Lenders Alliance

FTC and CFPB Actions against Payment Processors

Theories of Liability

- The processor intentionally facilitated fraud
- Turned a blind eye to red flags
- Processor provided substantial assistance to a person that violated consumer protection rules
- Processor is jointly and severally liable 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/executives

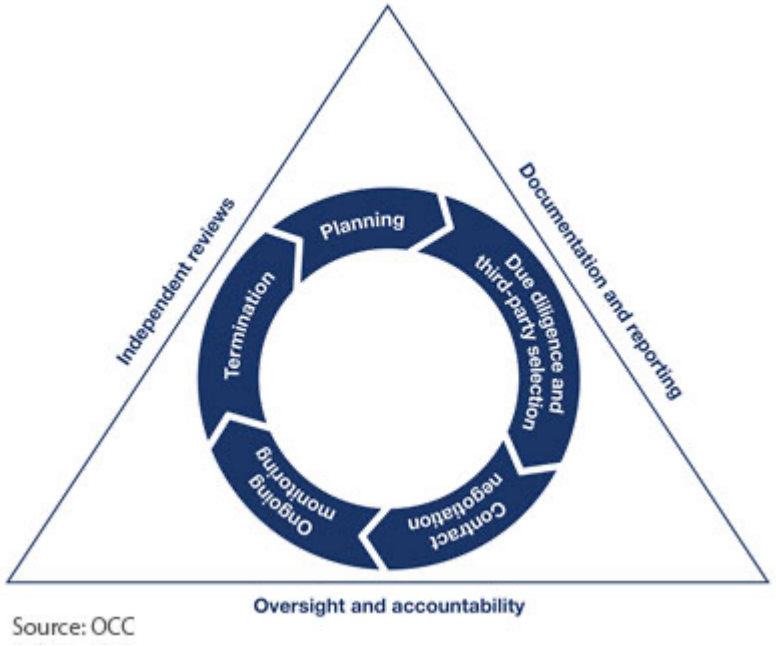
Common Settlement Terms

- Ban on operator as a processor
- Ban on servicing certain industries or merchants
- Merchant screening and monitoring requirements
- Civil money penalty
- Ongoing government oversight and compliance reporting

Interagency Guidance on Third-Party Relationships: Risk Management

- Released in June 2023
- Provides a harmonized view of safe and sound risk management for all stages of the life cycle of third-party relationships.
- 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."
- Guidance provides a lot of detail for the third-party selection and contract negotiation stages.
  - **BUT** ongoing monitoring may involve the most regulator attention/enforcement scrutiny.

Interagency Guidance on Third-Party Relationships: Risk Management



Source: OCC

Interagency Guidance on Third-Party Relationships: Risk Management

- Regulators 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 operation
  - Explicitly calls out third-party relationships "with new or novel structures and features – such as those observed in relationships with fintechs."

Interagency Guidance on Third-Party Relationships: Risk Management

- 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"
  - Maintaining oversight and accountability
    - Heavy board involvement
    - 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 and make adjustments as needed.
  - Documentation and reporting
    - At all stages of the lifecycle.

Interagency Guidance on Third-Party Relationships: Risk Management

- While third-party service providers may not be knowledgeable about the regulatory environment in which banks operate, they have access to sensitive information.
- State banks may have increased focus on third-party risk management of their fintech partners as the Interagency Guidance is more prescriptive and detailed than previous guidance.
- Contract negotiations between banks and fintechs will need to take into account the Interagency Guidance framework.

COMPLIANCE UNIVERSITY

OLA Online Lenders Alliance

Practical Tips for Third-Party Service Providers

- Understand regulatory requirements
  - Stay informed about the relevant regulations and compliance requirements in your industry.
- Third-party service providers should monitor their own service providers
  - Make sure you are engaging in appropriate third-party risk management practices and using the same methods to evaluate your service providers.
- Effective communication with your bank partner
  - Maintain open and transparent communication with your bank partner.
  - Schedule regular meetings to discuss compliance issues and updates.
  - Provide timely and accurate information to your bank partner.

COMPLIANCE UNIVERSITY

Online Lenders Alliance

Practical Tips for Third-Party Service Providers

- Establish effective risk management practices
  - Establish comprehensive compliance policies and procedures that align with regulatory requirements and make sure they are well documented.
  - Implement a robust risk management framework to identify, assess, and mitigate potential compliance risks and make sure they are regularly reviewed and updated.
  - Keep detailed and accurate records of all transactions, communications, and compliance-related activities.
- Training and Awareness
  - Conduct regular training sessions for your employees on compliance topics.
  - Employees should know the importance of compliance and their role in maintaining it.

Practical Tips for Third-Party Service Providers

- Monitoring and auditing
  - Establish ongoing monitoring and auditing processes to ensure compliance with all regulations and agreements.
  - Use internal and external audits to identify any gaps or areas for improvement.
- Utilize technology
  - Leverage technology to streamline compliance processes, such as using software for monitoring, reporting, and managing compliance data.

COMPLIANCE UNIVERSITY

Online Lenders Alliance

Drafting Considerations: Compliance with Applicable Laws and Regulation

Interagency Guidance	Practical Tips
• Specify the obligation of the third party and the bank to comply with applicable laws and regulations. • Ensure bank has right to monitor on an ongoing basis third party's compliance with applicable laws, regulations and policies and requires remediation if issues arise.	• When drafting your agreement, consider distinguishing between "Bank Applicable Law" vs "Service Provider Applicable Law." • Consider differentiating between applicable laws that are unique to each party's provision of services under the agreement.

COMPLIANCE UNIVERSITY

OLA Online Lenders Alliance

Drafting Considerations: Indemnification/Limits on Liability

Interagency Guidance	Practical Tips
• Specify the extent to which the bank will be held liable for claims or be reimbursed for damages based on the failure of the third party to perform. • Assess whether the limits on liability are in proportion to the amount of loss the banking might experience as a result of third-party failures, or whether indemnification clauses require the banking organization to hold the third party harmless from liability.	• Negotiate with a party by asking it to take risks within its control. • Which party has more consumer facing risk or liability?

Drafting Considerations: Default and Termination

Interagency Guidance	Practical Tips
• An effective contract stipulates what constitutes default, identifies remedies, allows opportunities to cure defaults, and establishes the circumstances and responsibilities for termination.	• Negotiate termination right for changes in applicable law. • Define "applicable law" broadly to include not just statutes and regulations but guidance, circulars, and interpretation of government authorities. • Exit rights if there are material adverse effects on either party or on the overall bank partnership program (e.g., reputational harm, litigation risk) • Provide for the timely return of the bank's data. • Assign all costs and obligations associated with transition and termination.

Drafting Considerations: Reality Check

- While regulator guidance identifies best practices, parties to a transaction are involved in commercial negotiations.
- The market will dictate how the parties will negotiate based on:
  - Who are the parties?
  - Who does what?
  - Who pays for what?
  - Who is in the best position to bear the risks?
  - What laws apply to which parties?

COMPLIANCE UNIVERSITY

OLA Online Lenders Alliance

Compliance Challenges with Artificial Intelligence

- Banking and financing industry is poised for a transformative shift thanks to AI.
- Regulators playing catch up on a technology with unique compliance risks.
- In recent FDIC exams, banks have been scrutinized for not being aware of the use of AI by their third-party service providers.
- A few compliance challenges for service providers that use or plan to use AI:
  - Complexity of AI systems
  - Staying on top of regulatory compliance
  - Bias and fairness concerns
  - Cybersecurity risks
  - Ethical AI

COMPLIANCE UNIVERSITY

Online Lenders Alliance

Compliance Challenges with Artificial Intelligence

- What are some compliance takeaways for service providers?
  - Transparency and reporting are critical. You should maintain open lines of communications with your bank partner on your use of AI and provide regular reporting on related risk management activities.
  - Ensure that you have a robust incident response plan, especially for AI-related issues or data breaches.
  - Continuously monitor your compliance with legal and regulatory requirements, including those related to AI.
  - Schedule regular audits and assessments.
  - Consider whether you want to include specific clauses in your contracts related to the use of AI to address transparency, accountability, and regulatory compliance.

COMPLIANCE UNIVERSITY

Online Lenders Alliance

Questions?

Mehul Madia

Sheppard, Mullin, Richter & Hampton, LLP

202.747.2301

mmadia@sheppardmullin.com

Max Bonici

Venable LLP

202.344.4832

mbonici@venable.com