Online Lenders Alliance

Are Your AML, ID Verification, and KYC Procedures Up To Date?

COMPLIANCE UNIVERSITY

OLA
Online Lenders Alliance

Presenters

Carlin McCrory
404.885.2740
carlin.mccrory@troutman.com

Matthew Bisanz
202.263.3434
mbisanz@mayerbrown.com

COMPLIANCE UNIVERSITY

COMPLIANCE UNIVERSITY

Online Lenders Alliance

Blue Ridge Consent Order

- January 2024 with the OCC.
- Previous agreement in 2022 regarding BSA/AML deficiencies in bank/fintech partnerships.
- The Bank has failed to establish and maintain a reasonably designed BSA/AML compliance program adequately covers the required BSA/AML program components. Deficiencies include: (i) systemic internal controls breakdowns, (ii) weak independent testing, and (iii) insufficient BSA staffing.
- The Bank has failed to correct problems in its BSA/AML Program that the OCC previously reported to the Bank relating to internal controls, independent testing, and BSA staffing.
- Additional findings relating to capital ratios, capital and strategic planning, and liquidity risk management.
- As with the prior regulatory action, Blue Ridge is prohibited from starting up any new third-party fintech relationships or building upon ones already started without the permission of the OCC.

Blue Ridge Consent Order Requirements

- Maintain a committee to monitor compliance with the order and regularly submit progress reports to the regulator.
- Submit a written plan to the OCC detailing how it intends to achieve and sustain BSA/AML compliance.
- Develop a written program to assess and manage risks posed by third-party relationships (discussed on next slide).
- Implement a BSA risk assessment program of the Bank's BSA compliance risk across all products, services, customers, entities, transaction types, countries or geographic locations of customers and transactions, accounts, and methods the Bank uses to interact with its customers, including activities provided through third-party relationships.
- Create a BSA audit program to test the Bank's compliance with the BSA relative to its risk profile, and the overall adequacy of the Bank's BSA/AML compliance program.

Blue Ridge Consent Order Requirements

- Ensure that the Bank has BSA personnel with requisite expertise, training, skills, and authority.
- Create a customer due diligence program to obtain and analyze appropriate customer due diligence, enhanced due diligence, and beneficial ownership information for all Bank customers at the time of account opening and on an ongoing basis.
- Develop a SAR monitoring and reporting program.
- Conduct a suspicious activity report lookback to determine whether SARs should be filed for any previously unreported suspicious activity.
- Create an IT control program.
- Develop a three-year strategic capital plan for achieving and maintaining capital no less than required by the order.

COMPLIANCE UNIVERSITY

Online Lenders Alliance

Blue Ridge Consent Order: Third-Party Relationships

Implement a third-party risk management program to comply with the interagency guidance on third-party relationships

The program must include, at a minimum:

- Written policies, procedures, and processes governing the Bank's third-party relationships;
- An assessment of BSA risk for each third-party relationship, including risk associated with BSA compliance, money laundering, terrorist financing, and sanctions risk, as well as each third-party relationship's processes for mitigating such risks and complying with applicable laws and regulations;
- Due diligence and risk assessment criteria for selecting and approving each third-party relationship that is appropriate and unique to the particular products, services, and activities provided by the third-party relationship;
- An effective compliance oversight program for third-party relationships;
- Ongoing monitoring of third-party relationship's activities and performance;
- Contingency plans for terminating third-party relationship in an effective and timely manner;
- Documentation, management information systems ("MIS"), and reporting that facilitates Board and management oversight, accountability, monitoring, and risk management associated with third-party relationships;
- An audit plan for independent reviews by a qualified auditor who is independent of day-to-day operations that allows Bank management to assess whether the Bank's risk management practices align with the Bank's policies, procedures, and processes. The audit plan must provide for effective independent reviews to assess internal controls as well as IT, compliance, and operational risk associated with third-party relationships;
- Evaluation and implementation of adequate staffing to manage third-party relationships, including personnel with the requisite expertise to oversee and manage the risks associated with each third-party relationship; and
- Full assessment of contracts with each third-party relationship to ensure the Bank's interests are protected.

Lineage Bank Consent Order – AML Requirements

- The FDIC ordered the bank to assess the resources needed to oversee AML/CFT functions at the Bank and provide for the designation of a qualified individual or individuals, with appropriate experience and training, responsible for coordinating and monitoring day-to-day compliance with the AML/CFT program.
- The individual is required to:
  - Have sufficient executive authority to monitor and ensure compliance with the applicable rules and regulations;
  - Report directly to the board of directors;
  - Report to the Bank's Audit Committee on a regular basis, not less than monthly, with respect to any AML/CFT matters;
  - Be responsible for assuring the proper filing of Currency Transaction Reports and Suspicious Activity Reports; and
  - Provide monthly comprehensive written reports to the board of directors.
- The Board must engage an independent, qualified third party to conduct a lookback of all activity from September 1, 2022 to the effective date of the Order for the largest FinTech partnership account to ensure any suspicious activities are identified, researched, and reported, as needed.

Preapproval requirements

- These and other enforcement actions have included a novel “preapproval requirement”
- The Bank shall refrain from onboarding any new FinTech partners or ACH end-customers via FinTech Partners until the Formal Onboarding Process has been submitted to the Regional Director for review and comment, approved by the Board, and thereafter implemented
- Bancorp shall not engage in any expansionary activities related to the fintech business strategy, including the establishment of any new subsidiaries, business lines, products, programs, services, customers, or program managers in connection with the fintech business strategy, without the prior written approval of the Reserve Bank

Preapproval requirements (cont.)

- The Bank shall not without the prior written approval of the Supervisors: (i) establish any new fintech partners, subsidiaries, business lines, products, programs, services, or program managers related to OBD, or (ii) offer new products, programs, or services to an existing fintech partner, program manager, or subsidiary of OBD. Before exiting a relationship with a fintech partner, the Bank shall conduct and provide the Supervisors with an impact analysis on the Bank's liquidity
- The Board shall review and approve risk tolerance thresholds for individual financial technology ("FinTech") partners based on an enterprise-wide financial analysis of each FinTech partner's financial projections under expected and adverse scenarios. The analysis shall include individual thresholds for each FinTech partner. Such analysis shall be provided to the Board to ensure tolerance thresholds are not exceeded

SSN Collection

- FinCEN generally requires banks to “obtain ... from the customer prior to opening an account ... [an] Identification number”
- Typically, a Social Security Number (SSN)
- Credit card providers may obtain SSN “from a third-party source prior to extending credit to the customer”
- Unclear if “Identification number” refers to the entire number or a portion of the number (i.e., the other portion can be obtain from another source)
- Fintech lenders have sought to comply by collecting only the last 4 digits from the customer and using a third-party source to obtain the rest
- Bank have increasingly been applying a strict requirement for their fintech partners to collect the full, nine-digit SSN directly from the customer at onboarding

Request for Information on SSN Collection

- In March 2024, FinCEN requested comment on potential changes to the SSN collection requirement and its interpretation of that requirement
- Could be read to imply that that the current interpretation is that banks (or their fintech partners) must collect the full, nine-digit SSN directly from the customer at onboarding
- Counterpoint is that the government and other authorities discourage customers to provide a full SSN for identity theft reasons
- Unclear if/when FinCEN will act on comments

Synapse Bankruptcy

- Synapse was a banking-as-a-service middleware company that connected fintechs with banks
- Fintech established a relationship with Synapse, which would maintain funds at banks for the fintech's customers and process related transactions
- Reduced need for fintechs to onboard at multiple banks and banks to onboard multiple fintechs
- Synapse did not establish a debtor-creditor relationship with customers, or have any relationship with the customer

Synapse Bankruptcy

- Synapse declared bankruptcy in April 2024 with the intent to sell itself to a third-party
- Synapse recognized a significant shortfall in its bank accounts for fintechs
- Alleged that shortfall was due to a fintech moving funds out of the bank accounts
- Listed ~100 creditors, including fintechs with 10 million customers
- Third-party terminated acquisition based on unresolved shortfall in Synapse's bank accounts

Synapse Bankruptcy

- Bankruptcy spiraled out of control due to Synapse's sudden and severe insolvency
- All employees were terminated in May 2024 and bankruptcy trustee has asserted that Synapse has no funds whatsoever
- Fintechs and banks lacked records to match (reconcile) transactions
- Some banks were used only to receive payments, while others made only disbursements
- Synapse did not clearly segregate funds per-fintech or from its own funds
- Customers could not obtain access to funds from fintech, Synapse, or bank
- Dispute as to whether customers have a relationship with any of the banks
- Bankruptcy judge asked federal banking regulators to intervene, but they declined, citing Synapse's status as a nonbank

Synapse Bankruptcy

- Synapse's banks subsequently worked with the bankruptcy trustee to reconcile fintech accounts
- Most funds have been returned to fintechs or their customers, but $85 million shortfall remains
- Tension exists as customers are not creditors of Synapse, but judge and trustee have a strong public interest in protecting customers from harm
- Trustee has struggled to retain service providers (e.g., forensic accountants, database providers) due to lack of funds and lack of institutional knowledge (e.g., passwords)
- Status of Synapse's lending and securities subsidiaries remains unresolved

Synapse Bankruptcy

- One of Synapse's banks received a consent order from the Federal Reserve in June 2024
- Stated that it was issued independent of the Synapse bankruptcy
- Cited deficiencies in the bank's relationships with fintechs, including with respect to risk management, anti-money laundering compliance, and consumer protection
- Requires bank to undertake extensive remediation efforts