Banking-as-a-Service Roles & Responsibilities Playbook

I Compliance & Regulatory Management

A. KYC, BSA/AML, and Fraud Monitoring

1. Program is responsible for implementing, maintaining, and monitoring systems that are adequate to ensure the Program's compliance with all Applicable Law pertaining to KYC, AML, BSA, and fraud monitoring.
2. Program is responsible for having proper, well-knowledgable staff, with an emphasis on legal and compliance within the leadership team.
3. Bank must approve procedures and may direct the Program to make changes to the procedures to bring them into compliance and regulatory guidance.
4. Bank is responsible for clearly outlining acceptable end clients, as well as prohibited businesses.
5. Bank will monitor all program activity with respect to BSA/AML enforcement.
6. Bank is responsible for monitoring transaction activity across all sponsored programs and determining when suspicious activity reports (SARs) are warranted and required under the BSA. Bank will file all SARs. Program will support Bank's investigations to support SAR decisioning.

B. Identity Theft Program

1. Program is responsible for developing and implementing an identity theft prevention program that is designed to detect, prevent, and mitigate identity theft.
2. Bank must approve the program.

C. OFAC Screening

1. Program is responsible for reviewing any false positive hits for OFAC, potential OFAC matches to determine whether hits are legitimate or false positives.
2. Program is responsible for closing accounts based on OFAC matches and retaining documentation for situations in which an account may remain open despite a positive or false positive match.

D. Program is responsible for implementing ongoing monitoring and testing protocols that test applicable regulations for compliance.

II Program Management

A. Bank shall maintain membership in at least two card networks.

B. Bank shall provide a clearly defined checklist and timeline to ensure rapid implementation of the Program

C. Program shall create account statements that are compliant with Regulation E. Regulation DD applies here as well

D. Bank shall provide and assist with tax reporting as needed (ex: statements, 1099, W-9 certifications, etc.)

E. Card Disclosures & Agreements

1. Program is responsible for creating the credit card and account agreements subject to Bank approval.
2. If Bank requests changes to the credit card agreement, Program is required to make those changes within an agreed upon timeframe. Bank should test that disclosures and agreements are delivered properly and are the approved version.

F. Terms & Conditions

1. Program shall provide Privacy Policy, Account Terms, Electronic Informed Consent and Conditions, and related disclosures to Customers.
2. The Bank has final authority over account terms and conditions, which may change from time to time based on legal requirements.

3. Bank will obtain Program's approval for account term changes unless they're required by law.
4. Program bears the cost of notifying customers of account term and condition changes.

G. Program shall contract and maintain a vendor to provide services related to external account verification.

1. Bank should provide an approved list of vendors when available.

H. Card Distribution

1. Bank must approve all card designs (including digital wallets) and card agreements.
2. Program ensures all cards are manufactured and shipped according to applicable law

I. Canceling Cards & Accounts

1. Bank may direct Program to terminate or cancel customer accounts of cards where it is determined to be necessary or advisable under law.
2. Program bears the cost of cancellation.
3. Program is responsible for returned card processing and will work with customer service on determining if customer should be contacted or Account closed.
4. Program will monitor for escheatment or dormant accounts.

J. Customer Service & Complaints

1. Program is responsible for handling customer service for their program and will prioritize adequate training and education for their staff.
2. Program shall manage all dispute resolution in accordance with network riles and Reg E and maintain records of all such complaints. Reg E complaint records must be provided to the Bank on request.
3. Program shall create a case management system to manage complaints that tracks and documents the Customer Complaint review and outcome. Program shall also develop a marketing management system to provide a like function.

III Governance

A. Operating Account

1. Program will maintain an operating account at the Bank that will be charged for reimbursable expenses.
2. Bank shall submit documentation evidencing reimbursable expenses each month.

B. Disaster Preparedness

1. Program to manage all Program servers, networks, devices (firewalls, switches, encryption devices, etc.) including back up and disaster recovery facilities to ensure the ongoing availability of the Program.
2. Both parties must develop and maintain disaster preparedness, recovery and business continuity plans.
3. Both parties shall periodically test their disaster recovery protocols and promptly provide the other party with the results.

C. Insurance

1. Program shall maintain comprehensive general liability insurance, commercial crime insurance, electronic data processing errors and omissions insurance, cyber liability insurance, and directors' and officers' liability insurance, each with policy limits that are at or above the ABA benchmark survey for coverages at similar sized financial institutions.
2. Policy limits can be below benchmark survey levels upon mutual agreement of both Parties.

IV Oversight

A. Data

1. Bank owns all customer account data. Regulatory agencies look very closely at this aspect; therefore the Bank is required to have adequate policies in place to maintain ownership of each account.
2. Program is granted use of customer data, owned by Bank. The Bank must have, maintain, and enforce data use policies.
3. Customers must legally opt in to allow their data to be shared with the Program. Banks must be prepared for audits proving shared customer data matches customer opt-ins.
4. Both parties will use customer account data solely to perform its duties under the agreement and shall not use customer data to market or sell.
5. After the termination of the agreement, both Bank and Program must maintain all records and documents for seven years.

B. Security Measures & Testing

1. Both parties will develop a comprehensive information security program to include regular penetration and vulnerability testing and policies, procedures and other measures designed to protect against unauthorized access to or use of Program customer account data.
2. In the event of a breach, each party will disclose the breach to the other.
3. Both parties are responsible for ensuring that third party service providers have similar, adequate security measures in place.

C. Public Announcements, Disclosures and Advertisements

1. All public announcements shall be approved by the other party in writing prior to release.
2. The parties shall each have a contractually determined amount of time to approve communications.
3. Program shall maintain all marketing materials in an electronic data site to which Bank will have continuous access.

D. Social Media Policy

1. Both parties must mutually lay out a social media marketing schedule that approximates the publishing date. Both parties are expected to provide feedback or approvals within a reasonable window.
2. Bank and Program will not publish material that is confidential or under copyright.
3. Bank and Program will not cite, reference, or interact with customers/clients/partners without both parties' approval.
4. Bank will provide Program with guidelines outlined by regulatory agencies, as well as the Bank's Endorsement Policy.
5. Program shall maintain all marketing materials in an electronic data site to which Bank will have continuous access.

E. Notifications

1. Each party is required to notify the other in the event of material adverse change in their business affairs that would be expected to affect the party's ability to fulfill the agreement.
2. Program shall notify bank in the case of filing SEC form D or prior to a change in control
3. Bank shall notify Program in the case of a supervisory objection to the Program from the Bank's regulators.
4. Each party shall advise the other of any data misappropriation, acts of money laundering, suspected terrorism, or fraud, and breaches, defaults, or terminations of third-party service providers and the reasons, therefore.

F. Third Parties

1. All service providers to the Program will be approved by the Bank so long as they meet its vendor management policies, suggested to complete via a service-level agreement.
2. Both the bank and the program shall develop and maintain a vendor management program, including vendor risk assessments.
3. Governance documentation for vendors to be provided and available to Bank

V Indemnification

A. Security Breaches - The party suffering an information security breach will reimburse the other party for costs of notifying customers so long as the breach resulted from the actions or omissions of the party suffering the breach or their contractors or employees.

B. Losses - Program indemnifies bank against all losses except for those caused by the Bank's own conduct or lack thereof.

VI Reporting

A. Financial records - Program shall provide Bank with its annual financial statements, balance sheets, and related statements of income and cash flow within 10 days of a request.

B. Audits

1. Each party shall coordinate its annual audits with the other and shall share their audit plans and engagement letters with one another.
2. Bank may conduct audits to ensure that the Program is being provided in accordance with the Agreement.

Appendix

List of Policies and Procedures

- Acceptable Use Policy
- Account Closing – Death & Bankruptcy Policy and Procedures
- Account Terms & Conditions
- ACH Policy, Procedures and Authorization
- ADA Policy
- Annual Fraud and Identity Report
- Audit Management Policy and Plan/Schedule
- BSA/AML/CIP/KYC & OFAC Policy, Procedures and Risk Assessment
- Change Management
- CIP (Customer Identification Policy)
- Code of Ethics
- Complaint Management Policy
- Compliance Management Policy and Procedures
- Compliance Training Program and Plan/Schedule
- Contact Center Guide
- Customer Complaint Policy and Procedures

- Data Retention Policy
- Disaster Recovery, Business Continuity Plan, Business Impact Analysis
- Dispute and Error Resolution Policy and Procedures (Reg E)
- E-Sign Consent Disclosure
- Elder Abuse Policy
- Error Resolution Disclosure
- Escheatment Policy and Procedures
- Fraud Policy
- Funds Availability Policy
- Governance documentation for vendors to be provided and available to Bank
- ID Theft Protection Program
- ID Theft Red Flags Risk Assessment
- Identity Program (including Digital/Device Intelligence)
- Inactive and Dormant Policy
- Information Security Policy
- IT Change Control and Approval Policy and Procedures
- Marketing Compliance Policy
- Mobile Banking Policy and Risk Assessment
- Physical Security Procedures
- Privacy Notice
- Privacy Policy
- Procedure documentation: Review/Investigation, Authentication – Auto or Manual, Lock/Block, Close, UAR

- Process Flows with Vendor Integration, Data Integrity Controls, and Decision Management (as relates to fraud): Onboarding, Funding, Money Movement, Non-Monetary Activity, Monitoring, Closure, Solution Alignment to Lifecycle Phase, etc. (updated annually or at significant modification)
- QA Process documented
- Record Retention Policy
- Red Flags Policy and Matrix
- Regulation E
- Risk Management Program Policy
- Strategy documentation
- Training related documentation
- UDAAP Policy, Procedure and Risk Assessment
- Vendor Management Policy, Procedures and Risk Assessment
- Wire Transfer Policy and Procedures

Alloy Labs is the only consortium that drives exponential growth for banks by leveraging network effects. Our members work together to identify opportunities for differentiation and co-create solutions that give them a competitive edge. In addition, they have exclusive access to The Concept Lab, a reverse accelerator that builds unique partnerships with startups, and the Alloy Alchemist Fund, which invests in the technology companies shaping the future of financial services. For more information visit www.alloylabs.com

Special thanks to the Alloy Labs member banks and industry leaders that participated in developing this playbook