cable

Bank-Fintech Guide: Financial Crime Diligence

When partner banks and fintechs enter partnerships, a key part of the diligence process covers risk and compliance topics. Regulatory guidance says, “During due diligence and before signing a contract, bank management should assess the risks posed by the relationship and understand the third party's risk management and control environment.”

This means banks need to collect sufficient information to understand who each fintech is and address operational needs, as well as documentation to evaluate the fintech’s risk and control processes.

Company Information

Banks should collect standardized general company information from all fintechs. This includes information for initial due diligence as well as critical operational information to ensure smooth communication throughout the relationship.

Common information requests include the following:

Critical Stakeholders

- ☐ Main point of contact (name, email, phone number)
- ☐ Designated signatory (name, email, phone number)
- ☐ BSA Officer/MLRO or Designated AML Officer (name, email, phone number)
- ☐ Chief Compliance or Risk Officer (name, email, phone number)
- ☐ Other relevant parties

Company Details

- ☐ Company legal name
- ☐ Company trading name
- ☐ Company address
- ☐ Company incorporation date and state
- ☐ Company registration or license number
- ☐ Company regulatory license status
- ☐ Number of employees
- ☐ Number of customers

Organizational Structure

- ☐ Beneficial owner details (name, date of birth, address, ownership percentage)
- ☐ Details of parent company

cable

Company Documentation

Banks should also collect standardized sets of policies, procedures, or other documents from all fintech programs to understand the fintech's risk and control environment.

Some fintechs, depending on their maturity, may not have all the documents readily available. In these cases, banks should seek an explanation from the fintech about the absence of the requested documents and determine if the fintech is within the bank's risk appetite.

Common document requests include the following:

Policies & Procedures

- ☐ Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) policy, and KYC/KYB, CDD, Identity Verification, Customer Risk Assessment, and EDD procedures
- ☐ Anti-Bribery and Corruption (ABC) policy
- ☐ Sanctions compliance policy
- ☐ Risk appetite statements
- ☐ Onboarding policies
- ☐ Terms of service or policies for declining applicants
- ☐ Financial crime controls register

Reporting & Self-Assessments

- ☐ Recent Board reports on financial crime compliance
- ☐ Recent financial crime audit reports
- ☐ Recent financial crime control review
- ☐ Recent financial crime risk assessments
- ☐ Recent financial crime key risk, performance, and control indicator reports
- ☐ Planned schedule of financial crime control reviews, audits, and risk assessments

Risk & Compliance Resources

- ☐ Diagram or description of corporate structure
- ☐ Diagram or description of compliance staffing
- ☐ Description of current financial crime compliance vendor relationships
- ☐ Financial crime compliance training materials and schedules
- ☐ Plans for any anticipated changes to systems or reporting capabilities