ABA Bank Compliance

MAY | JUNE 2023

Anti-Money Laundering/ Countering the Financing of Terrorism

The Opportunities and Challenges of Bank-Fintech Partnerships

BY DANIEL P. STIPANO, KENDALL HOWELL, AND CHARLES MARSHALL WILSON, II

OVER THE PAST DECADE, the products and services offered by fintechs have continued to expand, encompassing, among other things, personal financial management platforms, digital payments and mobile wallets, buy-now-pay-later financing, and credit scoring and lending based on alternative sources of data (www.cbinsights.com/research/report/top-fintech-startups-2022/). In turn, new business models, built upon partnerships between banks and fintechs (bank-fintech partnerships), have unbundled core banking activities—e.g., deposits, lending, and payments—and provided consumers with easy-to-use, online digital bank-like services and products (home.treasury.gov/system/files/136/Assessing-the-Impact-of-New-Entrant-Nonbank-Firms.pdf). Although bank-fintech partnerships can take many forms, the Banking-as-a-Service (BaaS) model is increasingly popular.

AML Considerations of Bank-Fintech Partnerships

BaaS typically involves a combination of a bank's infrastructure—such as its access to payment rails or ability to accept deposits—with technology developed by fintechs, resulting in efficient customer-facing services offered through digital platforms.(See www.federalreserve.gov/publications/files/community-bank-access-to-innovation-through-partnerships-202109.pdf.) BaaS relationships can be structured in a variety of ways: in some cases, banks and fintechs offer co-branded services to the bank's existing customers, while in others, fintechs offer services to consumers independently (often through accounts maintained at the bank). Through the BaaS model, fintechs and banks, working together, deliver a wide range of products, including peer-to-peer payments, online debit cards, and point-of-sale lending (www2.deloitte.com/content/dam/Deloitte/cn/Documents/financial-services/deloitte-cn-fsi-importance-of-banking-as-a-service-en-211019.pdf).

Key challenges, faced by both banks and fintechs, are anti-money laundering and countering the financing of terrorism (AML/CFT) risk mitigation and Bank Secrecy Act (BSA) compliance. Bank regulators are particularly focused on these areas. The AML/CFT compliance challenges presented by bank-fintech partnerships vary based on the nature of the relationship between the bank and its fintech partner, as well as the products, services, and activities offered through the partnership.

For example, where a bank's fintech partner is a regulated financial institution subject to the BSA and the fintech's activities are narrow in scope, effective AML/CFT risk mitigation may be more easily accomplished. Before entering into a partnership, banks and fintechs will want to assess the attendant risks, including the following:

- **Differing regulatory requirements for banks and fintechs.** A misalignment in regulatory requirements can result in conflicting compliance cultures, policies, and procedures between partners. For example, banks are subject to the Customer Identification Program (CIP)(31 C.F.R. § 1020.220), and Customer Due Diligence (CDD) Rules (31 C.F.R. § 1020.210(a)(2)(v) and 31 C.F.R. § 1010.230(a)), while fintechs are not. This may present challenges in identifying and sharing information regarding a fintech partner's customers.

- **Monitoring and mitigating risks effectively.** Risk oversight may be challenging based on the structure and nature of the bank-fintech partnership, especially where information is not freely shared between the bank and fintech.

- **Divergent business strategies and risk appetites.** Over the course of the partnership, evolving business strategies and risk tolerances can erode the effectiveness of risk mitigants and increase aggregate AML/CFT risks over time.

Before entering into partnerships, banks and fintechs must consider these risks, including how to mitigate and manage them, even if the BSA and its implementing regulations do not explicitly apply in certain cases.

During the diligence process, it is also important to evaluate the fintech's compliance program relative to the risk and volume of activity of the fintech's products, services, and customer types.

Regulatory Expectations and a Lesson Learned

The BSA requires financial institutions to establish AML/CFT compliance programs, which banks should, in practice, leverage to mitigate risk exposures that may arise in bank-fintech partnerships. Under the BSA and its implementing regulations, bank AML/CFT programs must include, at a minimum:

Internal controls designed to assure ongoing compliance with the BSA;

- A designated BSA officer;
- AML/CFT training for appropriate personnel;
- Independent testing for compliance with the BSA; and
- Risk-based procedures for conducting CDD, including:
  - Understanding the nature and purpose of customer relationships for the purpose of developing a customer risk profile; and
  - Conducting ongoing monitoring to identify and report suspicious transactions; and,
  - On a risk basis, to maintain and update customer information. (See 31 C.F.R. § 1020.210(a)).

In addition to these broad risk-based AML program requirements, the CIP Rule requires banks to implement procedures to verify the identity of their customers[1], and the CDD Rule requires banks to have written procedures that are reasonably designed to identify and verify the identities of the beneficial owners of their legal entity customers (31 C.F.R. § 1010.230(a)). Banks are also subject to other requirements under the BSA that may not be applicable to fintechs.[2] This misalignment in legal requirements applicable to banks and fintechs can create regulatory compliance challenges. For example, under the CIP Rule, regulators generally expect banks to collect all nine digits of a customer's social security number (SSN) if their SSN is their taxpayer identification number. However, fintechs are under no such requirement, and typically collect only the last four digits. However, as will be discussed, there are ways in which banks and fintechs can overcome compliance hurdles.

While the Financial Crimes Enforcement Network (FinCEN) has not released guidance specific to bank-fintech partnerships, banks are expected to implement risk-based procedures to mitigate AML/CFT risks across their enterprises (bsaaml.ffiec.gov/docs/manual/04_AssessingTheBSAAMLCompliancePrograM/01.pdf). This includes conducting risk-based due diligence on their customers which, in some cases, may include obtaining information on their fintech partners' customers or customer base (www.fincen.gov/sites/default/files/2020-08/FinCEN_Guidance_CDD_508_FINAL.pdf). In practice, it may be necessary for banks to conduct extensive diligence on their fintech partners to accurately assess and manage AML/CFT risks, in accordance with the CDD Rule and supervisory expectations generally.

In addition to their obligations under the BSA, banks that enter into partnerships with fintechs are expected to exercise effective third-party risk management (TPRM) to maintain safety and soundness and comply with legal requirements. In 2021, the federal banking agencies (FBAs) (i.e., the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, and the Office of the Comptroller of the Currency) issued proposed Interagency Guidance on Third-Party Relationships (Proposed TPRM Guidance). (See www.govinfo.gov/content/pkg/FR-2021-07-19/pdf/2021-15308.pdf.) The Proposed TPRM Guidance would establish a framework for TPRM that the FBAs would likely consider to be applicable to bank-fintech partnerships. Although the Proposed TPRM Guidance has not been finalized, it is reasonable to conclude that it represents the FBAs' views with respect to effective TPRM.

Lessons Learned from a Recent Enforcement Action

A recent settlement agreement between a bank and the Office of the Comptroller of the Currency (OCC) illustrates the BSA compliance expectations of regulators with respect to bank-fintech partnerships (www.occ.gov/static/enforcement-actions/ea2022-043.pdf). For example, the settlement agreement requires the bank to implement various AML/CFT risk mitigation measures, including:

- Implementing a BSA risk assessment program, which must ensure BSA compliance across all products, services, customers, entities, and geographies, including activities provided by or through third-party fintech partners;
- Adopting a revised BSA audit program that includes an expanded risk-based review of activities conducted through the

bank's third-party fintech relationships;
- Adopting and implementing improved policies, procedures, and processes to better obtain and maintain CDD, enhanced due diligence (EDD), and beneficial ownership information for all bank customers and third-parties, including third-party fintechs; and
- Implementing an enhanced suspicious activity monitoring and reporting program, which must timely identify, analyze, and monitor for suspicious activity across the bank, including activities provided by and through its third-party fintech partners.

The settlement agreement, along with statements and guidance from FinCEN and the FBAs, underscores that banks will be held responsible for addressing the risks associated with and resulting from bank-fintech partnerships, even if the BSA and its implementing regulations do not explicitly require them to do so. Accordingly, it is imperative that banks and their fintech partners work together to mitigate AML/CFT risks and promote BSA compliance.

Recommendations: Key Risk Management Considerations and Strategies

The settlement agreement provides a useful blueprint for BSA compliance in the context of bank-fintech partnerships; however, because banks are expected to take a risk-based approach to BSA compliance, appropriate TPRM and governance over bank-fintech partnerships will necessarily depend on the nature and scope of the partnership. The following controls and risk management principles will help banks and fintechs effectively manage AML/CFT risks associated with their partnership:
- Conducting risk assessments prior to entering into and over the course of a partnership;
- Performing initial and ongoing due diligence of fintech partners;
- Establishing and maintaining clear TPRM policies and procedures; and
- Contractually managing and allocating risks.

Risk Assessments

As a matter of both risk management and regulatory compliance, banks and fintechs are expected to understand their risk exposure arising from bank-fintech partnerships (www.occ.gov/static/enforcement-actions/ea2022-043.pdf). Although BSA regulations do not explicitly require financial institutions to conduct a risk assessment, FinCEN released an advance notice of proposed rulemaking in 2020 that, if finalized, would require financial institutions to conduct a risk assessment in order to achieve an effective and reasonably designed AML/CFT program (www.govinfo.gov/content/pkg/FR-2020-09-17/pdf/2020-20527.pdf).

The proposed rule has yet to be finalized, so although at the present time it is not an explicit legal requirement, banks and other financial institutions subject to the BSA are expected to conduct periodic risk assessments to identify AML/CFT risks across their enterprises.[3] The settlement agreement discussed above makes clear that this should include a comprehensive assessment of all activities provided by or through all bank-fintech partnerships.

Bank regulators will assuredly expect banks to conduct a full risk assessment of their fintech partners' products, services, customer bases, and activities prior to entering into formal relationships (www.federalregister.gov/documents/2021/07/19/2021-15308/proposed-interagency-guidance-on-third-party-relationships-risk-management). To ensure that information remains current and accurate, risk assessments should be refreshed on a periodic basis, as determined by each fintech partner's specific risk profile (www.occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html). Periodically updating risk assessments is of particular importance in the context of bank-fintech partnerships because many fintechs are in a dynamic state of growth and innovation, which may change the underlying risk profile of the partnership. In addition to risk assessments of individual bank-fintech partnerships, to identify risks at an institutional level, banks should also periodically assess their risk exposures across their bank-fintech partnerships as a whole. In all cases, banks must understand their risk appetite and adhere to that standard across all business relationships, including partnerships with fintechs.

A misalignment in regulatory requirements can result in conflicting compliance cultures, policies, and procedures between partners.

Initial and Ongoing Due Diligence

The BSA requires banks to conduct initial and ongoing due diligence on their customers, and bank regulators expect banks to conduct due diligence on third parties, including fintech partners (bsaaml.ffiec.gov/docs/manual/06_AssessingComplianceWithBSARegulatoryRequirements/02.pdf). Where a fintech is a bank's customer (i.e., it maintains a deposit or other account with a bank), the BSA requires banks to:
- Understand the nature and purpose of the customer relationship;
- Develop a risk profile;
- Maintain and update customer information (including beneficial ownership); and
- Collect sufficient information on the fintech and its end customers to Identify suspicious transactions (31 C.F.R. § 1020.210(a)(2)(v)).

In the settlement agreement, the OCC set forth a substantially more detailed set of due diligence expectations, indicating that banks should develop and fintechs should provide a complete understanding of their partners' operations, end customers, reporting and recordkeeping processes, and compliance procedures. Accordingly, regulators will likely expect banks to conduct due diligence both on their fintech partner's activities and on any services their fintech partners provide to their customers.

A key area of focus during the due diligence phase of a prospective partnership should be the partner's BSA/AML compliance program, specifically to assess the effectiveness of the program and to determine if the bank's and the fintech's compliance culture and risk appetite are aligned. Diligence in this area should cover, among other things, the partner's internal controls as well as the staffing, experience, and resources that comprise the partner's compliance function.

During the diligence process, it is also important to evaluate the fintech's compliance program relative to the risk and volume of activity of the fintech's products, services, and customer types. Where a fintech will rely on a bank's compliance infrastructure, it is equally important to conduct an internal assessment to determine whether the relationship is workable from a compliance perspective. For example, if the fintech conducts a large volume of high-risk transactions, and will rely on the bank for transaction monitoring, a bank must consider if its resources are sufficient to effectively monitor for and report suspicious activity.

Beyond compliance infrastructure and resources, due diligence should

examine how a partner's compliance function administers its policies. For instance, banks and fintechs should evaluate their partners' practices in managing high-risk customer types and addressing inaccuracies in customer documentation. Finally, banks' due diligence of fintech partners should cover processes and technology for monitoring and reporting suspicious activity. Among other things, banks should assess the compatibility of a fintech's transaction monitoring systems and processes, namely whether transaction data can be exported and integrated across systems.

AML/CFT and TPRM Policies and Procedures

Banks must establish clear, actionable policies and procedures that govern due diligence and ongoing monitoring of a fintech partnership. To ensure those policies are effective in practice, a bank should establish clear standards governing the diligence process, including the information that must be collected from fintech partners, the processes for approving partnerships, and the criteria for applying EDD. Similarly, a bank's internal controls should include specific standards and guidelines for evaluating fintechs' customer bases. Because many fintechs' products and activities evolve over time, it is also prudent to implement a change management policy that establishes controls that provide notice of material changes to a fintech's activities.

Regulators expect banks to maintain appropriate controls governing the suspicious activity reporting process, and thus, it is also important that banks and their fintech partners share information in a timely manner. To implement these policies effectively, it is important for banks and fintechs to train staff involved in all relevant aspects of the bank-fintech partnership—including both compliance and relationship management teams. Finally, banks and fintechs should establish and maintain governance policies and procedures that ensure that their boards and senior management are aligned.

Contractual Protections to Facilitate Compliance and Risk Management.

Once banks and fintechs decide to enter into partnerships, their respective management should negotiate a contract that clearly allocates BSA compliance responsibilities between the parties. These terms are not only an essential legal protection for banks and fintechs, but are also vital to ensuring ongoing BSA compliance. Under regulatory guidance, banks are generally expected to secure the right to audit a third party's compliance framework or the right to obtain copies of internal and external audits.

In addition, regulators would expect banks to secure broader rights to monitor and assess the adequacy of a fintech's AML/CFT controls on an ongoing basis. This may include the right to obtain records of independent testing of transaction monitoring systems (or the right to conduct such tests). Contracts should also establish detailed requirements governing information sharing and reporting. This should include, among other things, requirements to share information on suspicious transactions (including a detailed timeline for information sharing) and to provide updates on changes to a fintech's products, services, activities, or customers.

Banks and fintechs should also agree to representations, warranties, and/or covenants requiring ongoing compliance with the BSA or requirements to implement and maintain relevant AML/CFT internal controls. Contracts should also specify in detail the responsibilities of each party regarding BSA compliance. For example, where a fintech partner performs onboarding for shared customers, the fintech's role, responsibilities, and applicable compliance procedures with respect to AML/CFT should be clearly established by contract (e.g., in a Service Level Agreement).

Conclusion

AML/CFT compliance will continue to be an area of focus for regulators in bank-fintech partnerships and, as a consequence, banks and fintechs will need to dedicate resources to mitigate compliance risks. If banks and fintechs fail to meet their compliance and risk management obligations, there may also be supervisory and enforcement consequences. Notwithstanding, banks and fintechs may reasonably mitigate these risks by implementing and maintaining effective AML/CFT compliance programs; implementing and adhering to sound TPRM policies; and ensuring that compliance responsibilities are clearly allocated by contract. ■

ABOUT THE AUTHORS

DANIEL P. STIPANO is a Partner in the Financial Institutions Group at Davis Polk & Wardwell LLP. Reach him at **Dan.Stipano@davispolk.com**.

KENDALL HOWELL is an Associate in the Financial Institutions Group at Davis Polk & Wardwell LLP. Reach him at **Kendall.Howell@davispolk.com**.

CHARLES MARSHALL WILSON, II is an Associate in the Financial Institutions Group at Davis Polk & Wardwell LLP. Reach him at **Charles.Wilson@davispolk.com**.

ENDNOTES

1. See 31 C.F.R. § 1020.220(a)(2). In general, banks must obtain, at a minimum, the following information from the customer prior to opening an account: name, date of birth (for individuals), address, and identification number which, for U.S. persons, is their taxpayer identification number, 31 C.F.R. § 1020.220(a)(2)(i)(A)(1)-(4); and verify the customer's identity using documentary or non-documentary methods, 31 C.F.R. § 1020.220(a)(2)(ii)(A)-(B).
2. See, e.g., reports of transactions in currency, 31 C.F.R. § 1010.310-315; reports of suspicious transactions, 31 C.F.R. § 1020.320; due diligence programs for correspondent accounts for foreign financial institutions, 31 C.F.R. § 1020.610; due diligence programs for private banking accounts, 31 C.F.R. § 1020.620.
3. 31 C.F.R. § 1020.210(a)(2)(v); FFIEC BSA/AML Examination Manual, BSA/AML Risk Assessment (March 2020), https://bsaaml.ffiec.gov/docs/manual/03_BSAAMLRiskAssessment/01.pdf; FFIEC, FFIEC BSA/AML Examination Manual, Risks Associated with Money Laundering and Terrorist Financing: Third-Party Payment Processors – Overview (February 2015), https://bsaaml.ffiec.gov/docs/manual/09_RisksAssociatedWithMoneyLaunderingAndTerroristFinancing/11.pdf. Banks are similarly expected to conduct initial and periodic risk assessments of third parties.

ABA MEMBER RESOURCES

ABA bulletin: Anti money laundering
aba.com/news-research/email-bulletins/anti-money-laundering

Get certified: Certified Anti Money Laundering and Fraud Professional
aba.com/training-events/certifications/certified-aml-and-fraud-professional

Online training: BSA anti money laundering for compliance professionals
aba.com/training-events/online-training/bsa-anti-money-laundering-for-compliance-professionals

Podcast: How money mule tactics are evolving
bankingjournal.aba.com/2021/12/podcast-from-crypto-to-online-romance-how-money-mule-tactics-are-evolving/