Risk management redefined

Developing successful BaaS partnerships to limit financial crimes risk

January 2025

What is Banking as a Service?

Banking as a Service (BaaS)[1] is a business model where sponsoring banks[2] and platforms[3] can establish partnerships through a BaaS provider[4] to allow platform customers, such as merchants or individuals, to access various bank products or services through a streamlined user experience[5]. Consumer preferences have shifted to conducting business online rather than in person. Additionally, platforms have the ability to customize product offerings based on customers behaviors and perceived needs, which is made possible through the emergence of artificial intelligence. Both trends have contributed towards an explosion of BaaS partnerships over the past few years. BaaS partnerships allow nonbank businesses, such as tech firms, fintech companies, or retailers, to offer financial services without acquiring a banking license, while at the same time providing additional revenue opportunities for the sponsoring banks. In a typical BaaS model, as shown in *Figure 1* on the following page, a sponsoring bank holds the licenses required to offer various financial services, such as providing loans, issuing cards, managing deposits, and acquiring merchants. As a regulated financial institution under the Bank Secrecy Act (BSA), the sponsoring bank has the responsibility to abide by all anti-money-laundering (AML) and sanctions regulations.

The BaaS provider performs several roles including, but not limited to, matching sponsoring banks to platforms; supporting relationships with technology, such as application programming interfaces (APIs)[6]; and offering program management services, such as AML functions and other compliance services. Through this BaaS relationship, the platform leverages the license held by the sponsoring bank to offer financial products and services to their customers through one integrated platform without the need for their own bank charter, thereby benefiting from the established infrastructure and regulatory framework of the sponsoring bank.

[1] In the financial services industry, BaaS relationships are often referred to as bank-nonbank relationships.
[2] Sponsoring banks are often referred to as BaaS banks, partner banks, and financial institutions.
[3] Platforms are often referred to as fintechs, payments subsidiaries of technology companies, nonbank businesses, and third parties.
[4] BaaS providers are often referred to as pure BaaS providers, intermediaries, middlemen, or middleware firms.
[5] A BaaS relationship can also exist where there is no separate BaaS provider. For example, the sponsoring bank is one entity, and the other entity serves as the provider and the platform. In another example, there could be no BaaS provider, but rather the sponsoring bank uses their own infrastructure to integrate with the platform.
[6] APIs are a software code that includes rules or protocols, which enables software applications to access data and functionality.

Figure 1: Typical BaaS model

Typical BaaS model: Sponsoring bank, BaaS provider, and platform

Sponsoring bank

- Provides necessary licensing and regulatory approval through its charter
- Executes instructions received from the BaaS nonbank through the provider

BaaS provider

- Facilitates the relationship matching of BaaS banks and BaaS nonbanks
- Provides support of the BaaS relationship through their technology services (e.g., through APIs, ledgers, payment processing, etc.) to help the sponsoring bank and platform communicate and integrate
- Provides project management services, as requested
- Develops the API* to connect sponsoring bank and platform by integrating banking functions seamlessly
- Transfers instructions via the API for the platform to the sponsoring bank

Platform

- Offers products and services to its customers
- Maintains a front-end or user interface that allows its customers to interact with the financial products (e.g., bank accounts, cards, loans, etc.)
- Passes instructions to the sponsoring bank through the BaaS provider when there are interactions with the financial products

*Some sponsoring banks or platforms may offer their own APIs, but most typically rely on APIs built and managed by the BaaS provider.

Simplification of the symbiotic partnership

No doubt, BaaS partnerships offer many advantages for all parties engaged in these relationships. Benefits to the sponsoring bank include pipelines of new customers or entry into new geographic markets, scalability of operations, growth of bank deposits, and an increase in revenue. For the BaaS provider, the entire business model is driven by providing various services as the intermediary. The platforms benefit from the partnership as they can provide growth through new product and service offerings, accelerate time to market for new product/service offerings, promote growth of their user/customer base, increase revenue, and reduce overhead costs due to not having extensive regulatory obligations.

However, there are risk considerations that should be carefully considered and assessed by all parties prior to entering a BaaS partnership. From a regulatory perspective, a sponsoring bank outsourcing BSA/AML functions to a BaaS provider faces heightened risk of potential noncompliance with applicable laws and regulations and potentially increased costs driven by the need to dedicate resources to compliance oversight, including but not limited to due diligence and ongoing monitoring and testing of AML-related processes executed by third-party providers.

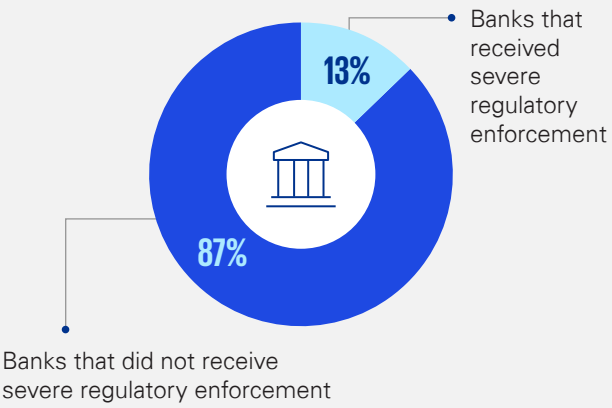
Sponsoring banks run the risk of developing unsustainable operating models and risk regulatory and reputational exposure through the facilitation of these partnerships. In the case of the platforms, the ease, speed, and agility that clients or users expect may be negatively impacted as the platform strives to comply with onboarding and compliance requirements set forth by regulations and enforced by sponsoring banks. AML-related compliance costs are also a factor for platforms to consider.

A rise in regulatory scrutiny surrounding BaaS partnerships

As previously outlined, one of the risks of a BaaS partnership is the increased regulatory risk and scrutiny that sponsoring banks may face. During 2023, only 3 percent[7] of banks engaged in BaaS relationships; however, these banks made up 13.5 percent of all severe[8] regulatory enforcement actions during that same year.[9] S&P Global noted there was an increase in BaaS partnerships,[10] which has led to heightened regulatory scrutiny at a seemingly disproportionate percentage. Moreover, the statistics could potentially understate the number of regulatory concerns as there may be sponsoring banks operating under Matters Requiring Immediate Attention (MRIA) and Matters Requiring Attention (MRA) related to BaaS relationships that are not part of publicly disclosed enforcement actions. When platforms or providers perform tasks other than Know Your Customer (KYC) collection, it may pose an increased amount of regulatory risk. But why is this?

Financial institutions have the responsibility to comply with AML and sanctions laws and regulations, including but not limited to requirements around collecting and monitoring KYC information, performing transaction monitoring to identify potentially suspicious activity, filing currency transaction reports and suspicious activity reports, performing sanctions screening for both customers and transactions, and many additional requirements. While the AML and sanctions compliance responsibilities may fall on the sponsoring bank, the sponsoring bank may not have necessary data or rights under the partnership to effectively monitor and oversee the various functions outsourced in BaaS relationships. Additionally, sponsoring banks tend to be small, community banks, which may not have the resources (e.g., inadequate number of full-time employees, inappropriate level of expertise, obsolete or inapplicable technology, etc.) to manage the risk. BaaS partnerships have the potential to vastly expand the sponsoring bank's client base and business volumes, seemingly overnight. The AML risks, of course, could see a commensurate rise. As such, the sponsoring bank may need to rely on the platform or BaaS providers (depending on the delegation of roles) to execute AML-related compliance functions, which may raise heightened risk for noncompliance.

Figure 2: US banks that received regulatory enforcement in 2023



The platform or BaaS provider may not provide an adequate amount of risk oversight (e.g., regular reporting of key risk indicators, issue management updates, etc.), have the appropriate level of expertise necessary to identify regulatory risks, nor have the same risk tolerance as the sponsoring bank. Further, the roles and requirements of the different players in BaaS relationships can be unclear, leading to potential breaches of regulatory compliance. For example, the onboarding practices at Sutton Bank's BaaS partners led to a Federal Deposit Insurance Corporation (FDIC) consent order.[11] The consent order required the bank to ensure compliance with Customer Identification Program (CIP) regulations by requiring "Prepaid Third-Party Program Managers" to collect the full first name of customers at account opening, test for compliance during the CIP testing process, develop procedures for identity verification, and conduct a lookback review of prepaid card customers onboarded during the past four years. When regulators identify compliance shortcomings, such as a lack of oversight resulting in noncompliance with BSA/AML requirements, the sponsoring bank bears the responsibility as the regulated financial institution.

[7] Thomas Mason and Yizhu Wang., "Small group of banking-as-a-service banks log big number of enforcement actions," S&P Global Market Intelligence (January 2024).
[8] S&P defined severe enforcement actions as prompt corrective action directives, cease and desist orders, consent orders, and formal agreements that were made public by federal regulatory agencies, including actions that were later terminated between January 1, 2020, and December 31, 2023.
[9] Thomas Mason and Yizhu Wang., "Small group of banking-as-a-service banks log big number of enforcement actions," S&P Global Market Intelligence (January 2024).
[10] Thomas Mason and Yizhu Wang., "Small group of banking-as-a-service banks log big number of enforcement actions," S&P Global Market Intelligence (January 2024).
[11] FDIC, "Consent Order: In the Matter of Sutton Bank, Federal Deposit Insurance Corporation" (February 1, 2024).

Banks involved in BaaS partnerships will often face regulatory scrutiny due to AML compliance oversight and other third-party risk management issues at their BaaS provider or platform partner.[12] For example, an FDIC consent order issued to Blue Ridge Bank, N.A.[13] highlighted several controls violations and issues in their BaaS operations. The key issues identified included:

1. **Inadequate monitoring of suspicious activity:** The bank failed to effectively monitor high-risk customer activity involving third-party fintech partners. This lack of oversight led to noncompliance with BSA/AML requirements.
2. **Deficiencies in third-party relationship management:** The bank's management of third-party relationships was found to be lacking. This included insufficient risk assessments, inadequate oversight, and failure to ensure compliance with regulatory requirements.
3. **Inadequate staffing and resources:** The bank was required to hire additional AML compliance officers and ensure appropriate staffing levels to manage the increased risk associated with their BaaS partnerships.
4. **Enhanced risk management program:** The consent order mandated the implementation of an enhanced risk management program overseen by the bank's board of directors. This included hiring a third party to assess risk management, increasing capital levels, and developing contingency plans for the termination of certain BaaS partnerships.
5. **Violations of Regulation E and DD:** The consent order cited specific violations of Regulation E (Electronic Fund Transfers) and Regulation DD (Truth in Savings Act). These violations indicated a failure to provide accurate and clear information to customers regarding their accounts and transactions.

In other instances, insufficient due diligence practices have resulted in several sponsoring banks not sufficiently addressing AML requirements and regulatory expectations, exposing them to regulatory actions and significant fines.

Effectively managing financial crimes risk in a BaaS relationship

Prior to engaging in a BaaS relationship, the chief compliance officer of the bank, along with senior management, at a minimum, should be involved in understanding the provider's and platform's services, customers, and the impact that entering into a BaaS relationship will have on its risk profile and the BSA/AML compliance and third-party risk management functions. In most cases, the platform's customers become the sponsoring bank's customers, so it is crucial for the sponsoring bank to understand the magnitude of risk presented by the platform and consider the nature of controls which may need to be implemented or enhanced to mitigate such risks. Thus, sponsoring banks should consider which roles, responsibilities, and risk mitigation control functions are outsourced to the BaaS provider or platform and the additional contract terms that are critical to establishing the roles and responsibilities of the parties. To reduce risk exposure, sponsoring banks may consider limiting the outsourcing of essential responsibilities. For instance, sponsoring banks may consider limiting the outsourcing of AML and sanctions compliance-related functions. Even functions such as record retention can lead to regulatory issues if not supported by clearly defined contractual obligations. The more roles that are outsourced to the BaaS provider or platform, the less control the sponsoring bank has over compliance-related functions, driving a need for increased oversight, which may prove challenging in outsourcing arrangements. Additionally, BaaS providers and platforms may not have employees with the requisite BSA/AML subject matter experience, which further increases the risk of noncompliance with regulatory requirements and expectations. Sponsoring banks should also require a risk assessment of both providers and platforms before entering into a BaaS partnership. Moreover, a sponsoring bank will need to know how to incorporate all the risks presented by the BaaS relationship into its own AML and sanctions risk assessment and customer risk rating model. A risk assessment should be a regular exercise for BaaS partnerships to promote due diligence and should focus on identifying key risks, assessing control gaps, and implementing risk mitigation measures. BaaS providers typically do not want to undertake performing risk assessments due to associated costs and resource constraints; so, it would behoove sponsoring banks to include risk assessments in contractual negotiations. Required risk assessments would improve identification of risks, an understanding of control deficiencies, and oversight of issue management, all from onset of the BaaS relationship.

[12] Other compliance concerns that arise due to BaaS partnerships include data privacy and security, which can lead to breaches of customer information and violations of privacy regulations.

[13] OCC, "Consent Order: In the Matter of Blue Ridge Bank, N.A., United States of America Department of the Treasury, Office of the Comptroller of the Currency" (January 24, 2024).

Throughout the lifecycle of the BaaS relationship, the sponsoring bank should contractually require information sharing between the sponsoring bank, platform, and BaaS partner to ensure the sponsoring bank's Board of Directors (BoD) regularly receive risk updates from the BaaS partners. It is essential for sponsoring banks to oversee risks. Additionally, they must report key performance and risk indicators to the bank's oversight function and senior management. Effective reporting includes trend analysis and reporting to highlight the significant risk and necessary risk mitigation efforts, which many sponsoring banks may not currently be adequately managing. Regular information sharing can assist in mitigating risks by increasing the visibility sponsoring banks have into platform and promoting potential issue identification, remediation, and validation. Additionally, sponsoring banks should stipulate that the BaaS provider have ongoing independent testing of outsourced AML and sanctions functions performed by qualified independent third parties. Independent tests should occur throughout the course of the relationship to identify vulnerabilities, prevent financial crimes, and mitigate concerns early, the results of which should be available to the sponsoring bank. Of course, all of these obligations of the sponsor and platform, as well as the bank, should be clearly established by the terms of the contract.

BaaS partnerships offer significant advantages, such as providing improved service offerings for merchants and individuals, a more streamlined user experience, and revenue growth. However, there are risks inherent in BaaS partnerships. Acting Comptroller of the Currency Michael Hsu stated that BaaS relationships can "create and distribute risk in unclear ways—with the public unwittingly expecting banks and bank regulators to cover problems no matter where they occur in the chain."[14] To promote management of AML-related risks, it is important to define strong roles and responsibilities, receive regular BoD reporting, and review risk assessments and independent testing reports. By partnering with reputable BaaS providers and effectively managing AML risks, banks can leverage BaaS partnerships to drive innovation, promote growth, increase revenue streams, and maintain the compliance standards that banking regulators demand.

[14] Source: OCC, "Size, Complexity, and Polarization in Banking" (July 17, 2024).

Contact us

Matthieu Chabelard
Principal, Forensic
Los Angeles, CA
KPMG LLP
917-513-4152
mchabelard@kpmg.com

Erik Krusch
Manager, Forensic
New York, NY
KPMG LLP
347-213-1571
ekrusch@kpmg.com

Patricia (Trish) Lee
Director, Forensic
New York, NY
KPMG LLP
917-242-5480
pvlee@kpmg.com

Jillian Brooks
Manager, Forensic
Denver, CO
KPMG LLP
973-975-7709
jillianbrooks@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

Learn about us: **kpmg.com**