Navigating AML compliance and regulatory challenges in BaaS

The better the question. The better the answer.
The better the world works.

EY
Shape the future with confidence

Introduction

Over the past two years, US federal financial regulatory agencies have expressed their focus on the compliance programs of institutions engaged in banking as a service (BaaS). Numerous consent orders issued by the Federal Reserve (Fed), the Office of the Comptroller of the Currency (OCC) and the Federal Deposit Insurance Corporation (FDIC) regarding banks' abilities to effectively manage the risks associated with their financial technology (FinTech) partnerships demonstrate the level of concern. Furthermore, the creation of specialized bodies to evaluate bank governance of BaaS arrangements, such as the Fed's Novel Activities Supervision Program and the OCC's Office of Financial Technology, as well as the issuance of BaaS-specific guidance, such as the "Interagency Guidance on Third-Party Relationships," indicate that sponsor banks offering financial services products through partnerships are under special scrutiny.

> "
>
> In 2024 alone, banks sponsoring the activities of FinTech companies represented approximately 2% of US banks,[1] yet they accounted for 18% of all enforcement actions issued by federal regulators.[2]

This number is expected to increase as regulators try to rein in BaaS banks. Notably, this mostly included banks with under $10 billion in assets, which have historically enjoyed relatively lower scrutiny, given a prevailing regulatory sentiment that these institutions posed lower financial crimes compliance (FCC) risk to the financial system.

These enforcement actions tend to focus on the sponsor banks' decentralized anti-money laundering (AML)/ countering the financing of terrorism (CFT) governance programs, differing approaches among FinTech partners for customer risk rating and alerts for potentially suspicious activity, and unaccounted risk factors within their AML risk assessment methodology. While this commentary within enforcement actions is not necessarily unique, BaaS models can present unique governance and data challenges, particularly for sub-$10 billion community banks where BaaS partnerships can potentially increase their customer base and transaction volumes to those more commonly seen among national and global financial institutions.

It is increasingly clear that regulatory agencies no longer evaluate sponsor banks using gradually heightened standards applied to asset size categories, which was historically taken as a proxy for a bank's complexity and risk. Given the nature of BaaS relationships, an institution's scale and operational complexity may not appear on the bank's balance sheet and are mainly driven by the transaction volumes and customer reach brought by their FinTech partners, with particular emphasis placed on the added complexity from the potential reliance on third parties to help manage aspects of the sponsor bank's risk. As regulators adjust their approach, sponsor banks accustomed to a perceived lower level of scrutiny will now see themselves held to standards historically applied to large global banks. Consequently, sponsor banks need to carefully consider the structure, framework and execution of their FCC programs. Sponsor banks must assume greater responsibility for their overall FCC strategies and integrate their FinTech customers into these programs in a more comprehensive manner. No longer can sponsor banks solely depend on their FinTech partners' compliance programs to fulfill the bank's regulatory obligations.

[1] "Small group of banking-as-a-service banks logs big number of enforcement actions," S&P Global Market Intelligence website, 23 January 2024, https://www.spglobal.com/market-intelligence/en/news-insights/articles/2024/1/small-group-of-banking-as-a-service-banks-logs-big-number-of-enforcement-actions-80067110.

[2] "BaaS is Not in Crisis: BaaS Banks Less Likely to Be Fined Than Non-BaaS Banks," Castellum.AI website, https://www.castellum.ai/insights/analysis-baas-enforcement-actions-2024.

AML challenges in the BaaS space

Recent enforcement actions provide insight into regulators' growing expectations. These actions consistently point to key themes and challenges that sponsor banks face, as they relate to their FCC programs:

Data governance: Sponsor banks can face significant data governance challenges, particularly where FinTech partners control the customer experience and the FinTechs don't provide their banks customer and transaction data timely or in the necessary format for the bank's risk and compliance obligations. Because the bank does not control the data, it needs to establish and enforce strict data requirements the FinTech must follow to normalize and transmit data in a manner consistent with the bank's data infrastructure and compliance systems.

Governance and board supervision: Because of its novel nature, a bank's legacy board might not have a thorough understanding of the risks associated with BaaS, so it is critical for compliance and Bank Secrecy Act (BSA) officers to explain the fundamental risks of third-party relationships. Regulators have focused their attention on banks keeping their boards informed on third-party risks via specialized committees and providing them with key performance indicators and key risk indicators.

AML and CFT compliance program and internal controls: Regulators continue to reiterate that banks are ultimately responsible for managing the risk associated with customers onboarded via their FinTech partners, regardless of whether FinTech partners execute compliance controls on the bank's behalf. Increasingly, regulators expect sponsor banks to establish risk and compliance standards, perform controls in-house or tightly govern the partner's compliance activities, and conduct monitoring and testing over the program, including any activities performed by the partner.

AML risk assessment: Along with consent orders for establishing a defined risk appetite, regulators have indicated through consent orders that sponsor banks need to consider their risk exposure from all banking activities, inclusive of their exposure based on the services offered by their FinTech partners. Regulatory sentiment has crystalized around the notion that FinTech partners are to be treated as an extension of the bank, operating as a de facto first-line business unit; therefore, they must be incorporated in the bank's risk assessments.

Transaction monitoring: Regulators are questioning sponsor banks' transaction monitoring programs along the following areas:

- **Effectiveness:** Increasingly, regulators are commenting on banks' lack of transaction monitoring rule coverage for risks identified through the risk assessment process.
- **Data quality and management:** Poor data quality and lack of availability continue to be central themes for sponsor banks among consent orders. Regulators expect sponsor banks to maintain ready access to the data necessary to fulfill transaction monitoring and investigations obligations, even if the data originates in the FinTech partners' systems.

Data quality and management: Poor data quality and lack of availability continue to be central themes for sponsor banks among consent orders. Regulators expect sponsor banks to maintain ready access to the data necessary to fulfill transaction monitoring and investigations obligations, even if the data originates in the FinTech partners' systems.

BSA and AML staffing and resources: Regulators have noted a risk with timely detection of AML risks and execution of controls in recent regulatory actions. They have also questioned whether banks truly understand the risks of the products and services their FinTech partners offer and whether they are appropriately staffed with the skills and resources to manage these risks.

This model, at a minimum, includes the following elements:

Building a more effective BaaS FCC program

For a sponsor bank's FCC program to be considered effective in this regulatory environment, the bank must operate with a model that (1) incorporates recent regulatory feedback; (2) improves its partner oversight; (3) integrates technology to assist in risk mitigation; and (4) establishes rigorous standards and enforces them through well-defined contracts, monitoring and testing, and robust communication between partner and sponsor.

Governance

Sponsor banks should enhance their third-party risk management frameworks by creating and enforcing governance programs that clearly delineate AML roles and responsibilities to reduce redundancy and promote complementary operations. This includes establishing a robust partner onboarding process documented via a compliance playbook or checklist to evaluate and integrate FinTech partners into the bank's AML operations. Banks must also establish clear requirements for FinTech partners, particularly if the FinTech partner (or a program manager) performs any AML controls on behalf of the bank. In the face of a more stringent regulatory environment, we have observed banks adding addenda or appendices to existing FinTech partner agreements to incorporate specific roles and responsibilities, control standards, data requirements, and service-level agreements (SLAs).

Furthermore, banks must have intimate knowledge of the AML activities their FinTech partners perform and be prepared to explain the delineation of duties between the bank and the partners to regulators. This level of transparency and accountability is essential for demonstrating control over all associated operations and maintaining the integrity of the BaaS ecosystem.

Tailored data controls and infrastructure

As referenced earlier, banks are accountable for maintaining compliance across all customer activity, including those onboarded via their FinTech partners. To meet compliance requirements, institutions need technology infrastructure and procedures to facilitate the timely transfer and processing of data from disparate sources (both internal and external), which is often a challenge. Strong data governance practices that facilitate streamlined data transfer are critical for sponsor banking relationships, and institutions should have defined partner onboarding and ongoing monitoring frameworks that include:

- Data format and content requirements, including minimum baseline standards of data required to facilitate monitoring
- Data quality standards to ensure accuracy and completeness
- Data transfer mechanisms and schedule of data transfer
- Description of the validations performed throughout ongoing data transfer to identify when standards are not being met, to drive conversations with partners
- Considerations for linking data across the ecosystem, where customers may have relationships across multiple partners

As sponsor banks expand their partnerships with FinTech companies, it's crucial for them to steer clear of provisional data solutions that necessitate manual handling or reconciliation. Sponsor banks should also carefully assess the data implications when choosing essential vendors for their FCC programs, such as screening providers, to establish proper integrations and configurations for efficient data utilization.

AML risk assessment

In light of recent enforcement actions, as well as the Financial Crimes Enforcement Network (FinCEN) Notice of Proposed Rulemaking issued on June 28, 2024, which seeks to codify the AML risk assessment process as a program requirement, sponsor banks should focus on enhancing their overall risk assessment process. This process should include a detailed methodology to support consistent and repeatable assessments across the bank (inclusive of traditional bank lines of business and each FinTech partner), based on the bank's customers, products, services, transactions, geographic exposure and distribution channels. Assessments should incorporate the FinTech partners' business models and product offerings supported through the bank and should provide the bank with an understanding of incremental financial crime risks introduced by each FinTech, alongside the bank's controls and mitigating factors. The results of the risk assessment should incorporate insights gained from regulatory reporting (e.g., suspicious activity reporting, currency transaction reporting), information-sharing processes, and the AML/CFT Priorities published by FinCEN.

The AML risk assessment process should serve as the foundation for strategic and business decision-making, such as the allocation of resources for compliance operations (e.g., monitoring, testing, enhanced due diligence (EDD)). Sponsor banks should leverage the risk assessment to evaluate overall risk exposure when considering the impact of a new FinTech partnership or managing existing partners, particularly as they explore expansion into new customer segments or product offerings.

Transparent communication protocols and change management processes

Sponsor banks should establish channels and processes for their FinTech partners to inform them of high-risk activity as well as changes to their business model that may expose the bank to new risks or require a recalibration of existing controls, such as the introduction of new products and services or supported transaction types, or the expansion into new markets. The sponsoring bank can support escalation of changes by implementing change management processes (e.g., change identification, impact, processes to enhance the control framework) and the scheduled revision of SLAs. As noted above, banks must define the standards by which their FinTech partner must communicate potential changes, define the process to assess risks and approve requested changes, and incorporate necessary program enhancements to offset changes in risk.

Consistent customer risk rating approach

Inconsistency in customer risk ratings (CRR) between sponsor banks and FinTech partners can lead to confusion in the appropriate application of downstream AML controls. For example, a customer deemed high risk by the sponsoring bank but considered medium risk by the onboarding FinTech may not be subjected to advanced processes, such as EDD or requests for information, even if the FinTech follows the bank's onboarding procedures. Therefore, sponsor banks must enforce adherence to their CRR standards to promote consistency in approach to, and mitigation of, AML risk.

Testing requirements to verify the alignment between bank and FinTech AML programs

As regulators have continued to highlight in recent regulatory actions, BaaS institutions maintain ultimate responsibility for their FCC programs, including where FinTechs perform AML controls on behalf of the bank (e.g., customer identification program (CIP), know your customer (KYC)). Banks are responsible for developing and disseminating standards for execution, and documenting policies and procedures to periodically test to verify that the FinTech is meeting performance and effectiveness expectations. The testing program should include a review of operational processes but should also focus on review of outputs from monitoring and investigations (e.g., validation of CIP collection and KYC reviews at onboarding).

The testing program should also detail remedial activities that may be required if there are findings identified during testing, which may include requiring the FinTech to implement enhanced controls, closer cooperation between the FinTech and the bank's AML team, more frequent or expanded testing, review and confirmation that findings have been addressed, and potential penalties or actions taken if there is a failure to remediate. Importantly, potential consequences or penalty measures should be contemplated in sponsor banks' agreements with their FinTech partners, providing a contractual mechanism to drive accountability when the bank identifies an issue requiring correction.

Transaction monitoring

Transaction monitoring systems are critical for institutions to detect and report suspicious activity; however, particularly in the BaaS domain, there is no one-size-fits-all transaction monitoring approach or system. As a result, institutions should consider the following when designing and implementing transaction monitoring programs:

- Each of the FinTech partners often has a unique and nuanced customer or end-user population with its own risk profile.
- Products offered by FinTechs can be complex and vary significantly from partner to partner, and from the core bank, necessitating tailored monitoring rules.
- When managing relationships with a large number of FinTech partners, the rate at which new products are requested for launch increases significantly compared to traditional commercial and retail banking.
- Data required for monitoring comes from many disparate upstream sources (e.g., different payment processors used by each FinTech), often with differing levels of quality, standardization and availability.

While many sponsor banks once depended on their FinTech partners to perform at least some form of transaction surveillance, evolving regulatory expectations have driven a shift toward the bank performing these activities (except in cases of fraud detection, which often is best performed by FinTechs given their proximity to the customer and ability to stop payments in real time). This change allows sponsor banks to assume direct responsibility and control over the detection and investigation of potentially suspicious activity in a consistent manner.

Sufficient and skilled staffing

Sponsor banks can benefit from performing resource assessments on a recurring basis to evaluate whether both the bank and their FinTech partners have the capacity and skill sets to effectively execute AML controls. If banks find their current resources do not have the scalability to manage the evolving risk profile, they should consider alternative staffing models.

Based on EY teams' experience working with BaaS institutions, we have observed significant challenges in the ability to scale their compliance operations due to increased volumes from FinTech partner activities. Sponsor banks can achieve this scale more easily by leveraging service providers who can help them accomplish the following:

1. **Focus on business-as-usual (BAU) operations:** By outsourcing manual or time-consuming AML operational functions, financial institutions can concentrate their resources and efforts on higher-value activities and strategic initiatives, which can enhance productivity and overall AML risk management capabilities.

2. **Cost efficiency:** Financial institutions can reduce operational expenses by outsourcing certain AML program activities to specialized providers rather than maintaining full-time or in-house teams. This can lead to savings on labor, training and infrastructure over time and provide banks with needed flexibility in their resource models to manage elastic volume. Furthermore, where firms can quantify their cost of compliance, or unit-based costs associated with an activity (e.g., triage of a Level 1 transaction monitoring alert, Level 2 case investigation), they can begin to discuss those costs of compliance with their FinTech partners and discuss how to more appropriately share in those costs as part of their commercial arrangements.

3. **Specialization:** Managed service providers can bring knowledge and experience that may go beyond the scope of internal capabilities, providing high-quality service and skill sets that could prove difficult to cost-efficiently replicate in-house. This gives financial institutions the flexibility to scale their managed services up or down to address variability in volumes stemming from ebbs and flows in partner activity.

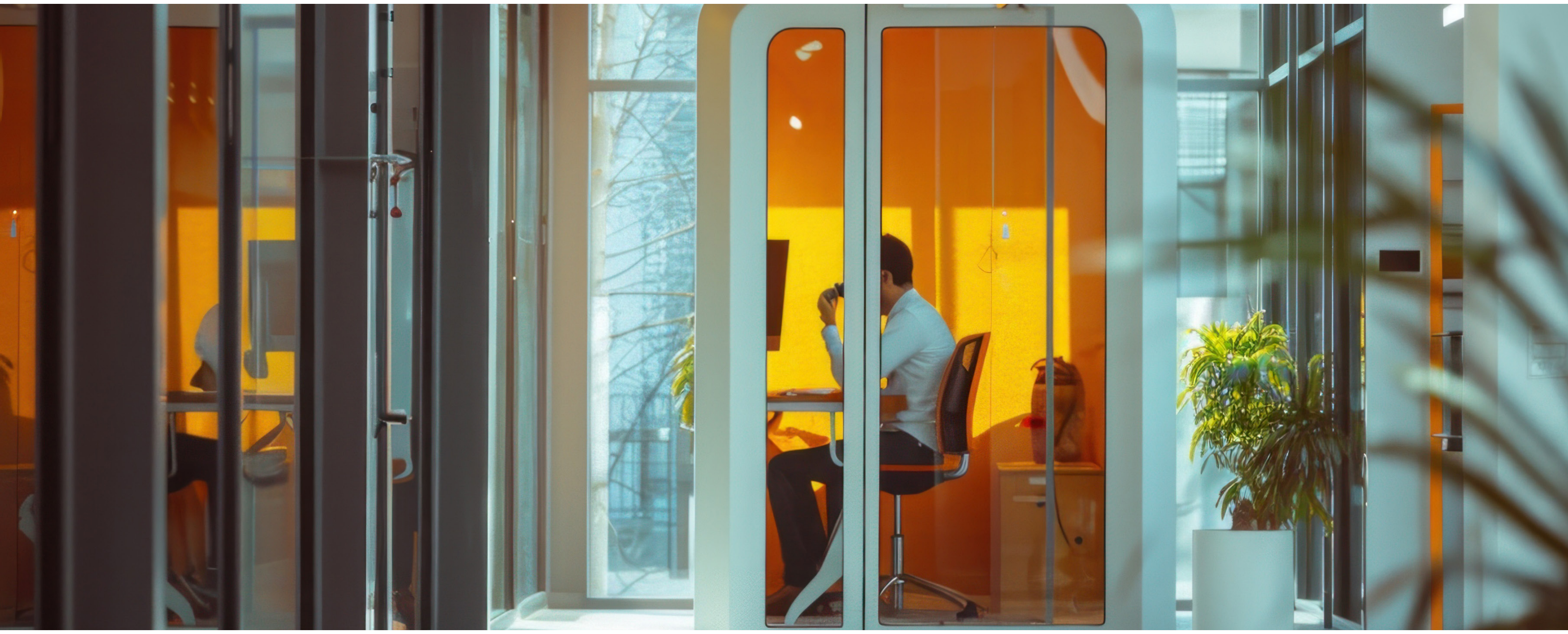
Conclusion

Based on EY teams' experiences assisting banks with their BaaS programs, many institutions we have spoken with are uncertain about how to effectively meet their regulatory requirements in the current environment. Considering recent regulatory enforcement trends, banks and FinTech partners should aim to enhance their AML programs by taking the following actions:

- Establish robust governance programs and clear AML roles and responsibilities for FinTech partners.
- Enhance the AML risk assessment process to ensure consistent and repeatable evaluations across all business lines and FinTech partners.
- Implement transparent communication channels and change management processes for FinTech partners to report high-risk activities and business model changes.
- Ensure FinTech partners use the same customer risk rating model to maintain the effectiveness of AML controls.
- Develop strong data governance practices and ensure seamless data transfer and quality standards with FinTech partners.
- Periodically test FinTech partners' AML controls and document policies for remedial actions if necessary.
- Design and implement tailored transaction monitoring programs to detect and report suspicious activities effectively.
- Perform regular resource assessments and consider alternative staffing models to ensure adequate capacity and expertise for AML operations.

By proactively addressing these areas, BaaS-sponsor banks can better position themselves to navigate the evolving regulatory landscape and maintain robust, effective AML programs that support their current and future business needs and strategy.

EY teams have served both FinTechs and BaaS banks across the maturity spectrum on regulatory remediation, redesign of risk and compliance program frameworks, development of specific compliance program elements to oversee BaaS partner compliance, cost-effective and scalable operations, and designing strategies for addressing risks associated with onboarding new partners. We bring this industry perspective, along with a versatile roster of professionals experienced in helping interpret, respond to and prepare for regulatory examinations. Contact us to learn more about how we can support your BaaS journey.



Key Ernst & Young LLP contacts

Michael Winter
Principal
Ernst & Young LLP
michael.winter@ey.com
+1 415 894 4244

Andrew Abdalla
Senior Manager
Ernst & Young LLP
andrew.abdalla@ey.com
+1 415 486 3608

Sam Holt
Senior Manager
Ernst & Young LLP
sam.holt@ey.com
+1 206 654 7613

Meggaen Neely
Senior Manager
Ernst & Young LLP
meggaen.neely@ey.com
+1 979 239 8106

Gabriel Toledo Guerrero
Manager
Ernst & Young LLP
gabriel.toledo.guerrero@ey.com
+1 212 466 9459

Christine Dorband
Manager
Ernst & Young LLP
christine.dorband@ey.com
+1 312 879 4286

EY | Building a better working world

EY is building a better working world by creating new value for clients, people, society and the planet, while building trust in capital markets.

Enabled by data, AI and advanced technology, EY teams help clients shape the future with confidence and develop answers for the most pressing issues of today and tomorrow.

EY teams work across a full spectrum of services in assurance, consulting, tax, strategy and transactions. Fueled by sector insights, a globally connected, multi-disciplinary network and diverse ecosystem partners, EY teams can provide services in more than 150 countries and territories.

All in to shape the future with confidence.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. EY member firms do not practice law where prohibited by local laws. For more information about our organization, please visit ey.com.

Ernst & Young LLP is a client-serving member firm of Ernst & Young Global Limited operating in the US.

© 2025 Ernst & Young LLP.
All Rights Reserved.

2502-10155-CS
ED None
US SCORE no. 26748-251US

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, legal or other professional advice. Please refer to your advisors for specific advice.

ey.com