Building a better working world

Complying together

Enabling Banking as a Service via the anti-money laundering program

Banks provide Banking as a Service (BaaS) to partner organizations to generate new revenue streams, expand distribution channels and increase the size of their customer base. These partners are often financial technology companies (FinTechs). The banks provide core financial products to their partners such as checking and deposit accounts, credit cards and loans. The partners in turn provide these products to their customers without having to build a banking infrastructure or acquire a banking license.

Recently, regulators have become increasingly interested in BaaS. Regulators have noted that they have seen a rise in banks, particularly regional and community banks, partnering with FinTechs. The Office of the Comptroller of the Currency (OCC) indicated that it sees these relationships presenting potentially new inherent risks. Notably Michael Hsu, Acting Comptroller of the Currency, in September provided the following quotes indicating perhaps greater regulatory scrutiny over these relationships going forward:[1]

"I believe FinTechs and big tech are having a large impact and warrant much more of our attention."

"The growth of the FinTech industry, of Banking as a Service, and of big tech forays into payments and lending is changing banking, and its risk profile, in profound ways."

"At the OCC, we are currently working on a process to subdivide bank-FinTech arrangements into cohorts with similar safety and soundness risk profiles and attributes. This will enable a clearer focus on risks and risk management expectations."

[1]Acting Comptroller of the Currency Michael J. Hsu, Remarks at the TCH + BPI Annual Conference, "Safeguarding Trust in Banking: An Update," September 7, 2022. www.occ.gov/news-issuances/speeches/2022/pub-speech-2022-106.pdf

In our experience working with both banks and their partners, we are aware many have received feedback on topics such as clearly defining roles and responsibilities for anti-money laundering (AML) controls across the bank and its partners; having a robust and clearly documented customer risk scoring methodology that can monitor risks of the expanding customer base; and providing detailed guidelines for assessing transactional activity in customer accounts, especially with higher-risk transaction types such as international wires and peer-to-peer (P2P) payments.

BaaS arrangements present unique challenges with performing two vital aspects of an AML program: Know Your Customer (KYC) checks and monitoring transactions. **The following example illustrates this challenge.**

- Partner ABC collects the following information on its customers: name, date of birth, taxpayer identification number and expected activity. Partner ABC also collects the following transaction information: originator, beneficiary, date and amount. All of this information is shared with Partner ABC's bank via solution 123.

- Partner XYZ collects name, date of birth, taxpayer identification number and occupation. Partner XYZ also collects the following transaction information: originator, beneficiary, date, amount and countries involved. Partner XYZ shares the customer information with its bank via solution 789 and shares the transaction information via solution 456.

The example illustrates that the information that is passed from the partner to the bank and how the information is passed is different across partners. **This leads to the following questions:**

- How can the bank demonstrate that it is comfortable with the partner's risk profile and has controls in place to mitigate the risk?
- How will the bank perform consistent and effective customer risk scoring?
- How can the bank demonstrate that it knows the customer?
- How will consistent and effective transaction monitoring occur?

Without the proper infrastructure, partnership agreements and AML controls in place, these differences will impact the bank's ability to adhere to AML regulations.

The inherent money laundering risks can be mitigated by a thoughtful operating model between the bank and its partners. We examine this operating model through the following areas: risk assessment, data, KYC, transaction monitoring, and governance and oversight. Creating an operating agreement and fee structure in which the costs of the operating model are shared between the bank and partner is important.

The first step the bank should take is understanding the risk profile of the BaaS partner through a documented risk assessment. The BaaS arrangement will expand the bank's customer base and geographic footprint, potentially impacting the bank's risk profile. The bank can provide financial products to one partner that are different from those provided to another partner. The risk assessment should clearly document the inherent risks presented by the partner, the mitigating factors, controls, and the residual risk after the mitigating factors and controls have been applied. A critical part of the risk assessment is to understand the impact the partners' customers and transaction activity will have on the bank's AML operations. The bank will need to determine if the residual risk is within its risk appetite parameters and whether the bank can handle the operational impact. The framework to assess the partner's risk should be consistent, reviewing the underlying products and customers across partners, but the residual risk outcomes can be quite different. Then, as the bank and partner continue their relationship, the bank should perform, at a minimum, annual enhanced due diligence reviews of the partner to reassess the risk profile and determine whether it remains within the bank's risk appetite.

Regulators are holding banks accountable to comply with AML regulations. However, partners collect and provide data to the banks to perform AML functions. There is no industry standard for the format or method of sharing data between partners and banks. This lack of standardization results in inconsistent and incomplete data provided to banks. A second common challenge is that banks may not have enough insight into the partner's

> BaaS allows both the partners and banks to experience rapid growth in the customer base. The resulting impact to the AML program can be just as significant.

data (e.g., which customers are deemed high risk by the partner, which accounts have been closed by the partner). Incomplete or unclear data can hinder the bank's ability to carry out its AML responsibilities effectively and to evaluate risk.

Banks and their partners need to work closely together to develop data requirements and infrastructure, including:

- Agreement on required data and format to which partners must adhere. The requirements can be documented in the contract between the bank and partner, the partner's contracts with its customers, the partner's procedures for onboarding customers, and in the partner's data and system architecture documentation.
- The process by which banks and partners can request new data need to be defined, along with a corresponding service level agreement (SLA) for implementation.
- The infrastructure for how the partner's data is integrated into the bank's AML systems.
- Testing requirements for new products and services or other new requirements before implementation.

Often banks will need to create a data mart that receives all partners' data. From this data mart, partner data is converted into a common format that is fed into the bank's AML systems.

Another important aspect is defining the process and channels by which the partner updates the bank on any changes to its business (e.g., new product, customer type, market). There should be an SLA in place that sets the timeline for the partner to share the conceptual change to the business with the bank before the change is implemented. The bank and the partner will then need a mutually agreed-upon timeline for updating AML controls to address the change prior to implementation.

The bank and the partner need to define clear roles and responsibilities prior to entering into a BaaS relationship. Will the bank essentially perform all aspects for the AML program, or will there be split responsibilities for both the bank and partner to perform? Perhaps the partner performs level 1 transaction monitoring alert reviews and the bank performs level 2 case investigations and SAR filing. If so, how will the results from the level 1 investigation feed into the bank's level 2 case management tool? How will changes to the transaction monitoring program be governed? How will the feedback loop from the bank to the partner occur? Will the bank be able to audit the partner's AML program or perform sample testing?

Regardless of the distribution of controls, there will be instances in which banks require additional information from the partners to perform AML controls. These processes and associated communication channels need to be clearly documented before entering into the BaaS relationship, including any technology requirements needed at the outset. For example, with transaction monitoring and enhanced due diligence, the bank's AML staff may need to submit requests for information to the partners, either for the partners to address or to contact their customers. Relatedly, banks and partners must agree on record management and retention policies to support internal and external audits and examinations.

Resourcing can be a challenge for banks and partners as well. As noted, BaaS allows both partners and banks to experience rapid growth in the customer base. The resulting impact to the AML program can be just as significant, requiring a surge in resourcing to support new controls (e.g., enhanced due diligence on partners) as well as maintain the increasing volume of existing controls (e.g., transaction monitoring, enhanced due diligence

on partner's customers). As banks and partners consider a BaaS relationship, both institutions should consider leveraging strategic cost efficiencies with respect to resourcing and technology to enable the BaaS growth.

Based on our experience with assisting banks with BaaS, we have seen significant change in banks' AML programs and growth in AML staff to address the complexities mentioned above. For example, banks are considering customer risk scoring models that assess the underlying customers and products across partners, moving away from models that viewed each partner independently. Also, as banks and partners grow in this space, they are looking to automation and third-party support (managed services) to augment their growth.

So what should banks and partners be doing, either as they begin their journey with BaaS or navigate this unique and complex arrangement?

Engage key stakeholders

Banks and partners need to build an operating model together that considers people, processes, data and technology, which allows the BaaS partnership to scale. Through collaboration, banks and partners can avoid certain pitfalls outlined above. Also, regulators should be engaged to cultivate transparency and receive constructive feedback on the operating model while mitigating the risk of potential future findings.

Assess current data architecture

Evaluate the existing data architecture and the ability to change it to address the needs identified for the BaaS relationship. This evaluation should include all data currently collected (customers, transactions, etc.) and system integrations both internally and externally.

Look for cost efficiencies

A BaaS relationship can require significant growth in the AML program, leading to an increase in spending to remediate or enhance AML controls. In addition to sharing the cost across the banks and partners, institutions should look for other ways to supplement the AML program's growth, such as robotic process automation, managed services, third-party data usage and tools to streamline risk assessments and customer risk scoring.

EY teams lead the industry in providing anti-money laundering and sanctions compliance, risk and technology advisory services to financial institutions, financial technology firms and other industries. To learn more about our experience, please reach out to any of the following subject-matter advisors.

Don Johnson
Principal
Ernst & Young LLP
donald.johnson@ey.com

Christopher Dillon
Managing Director
Ernst & Young LLP
christopher.dillon@ey.com

Meggaen Neely
Senior Manager
Ernst & Young LLP
meggaen.neely@ey.com

EY | Building a better working world

EY exists to build a better working world, helping to create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

2210-4121716
ED None
SCORE no. 18669-231US

ey.com