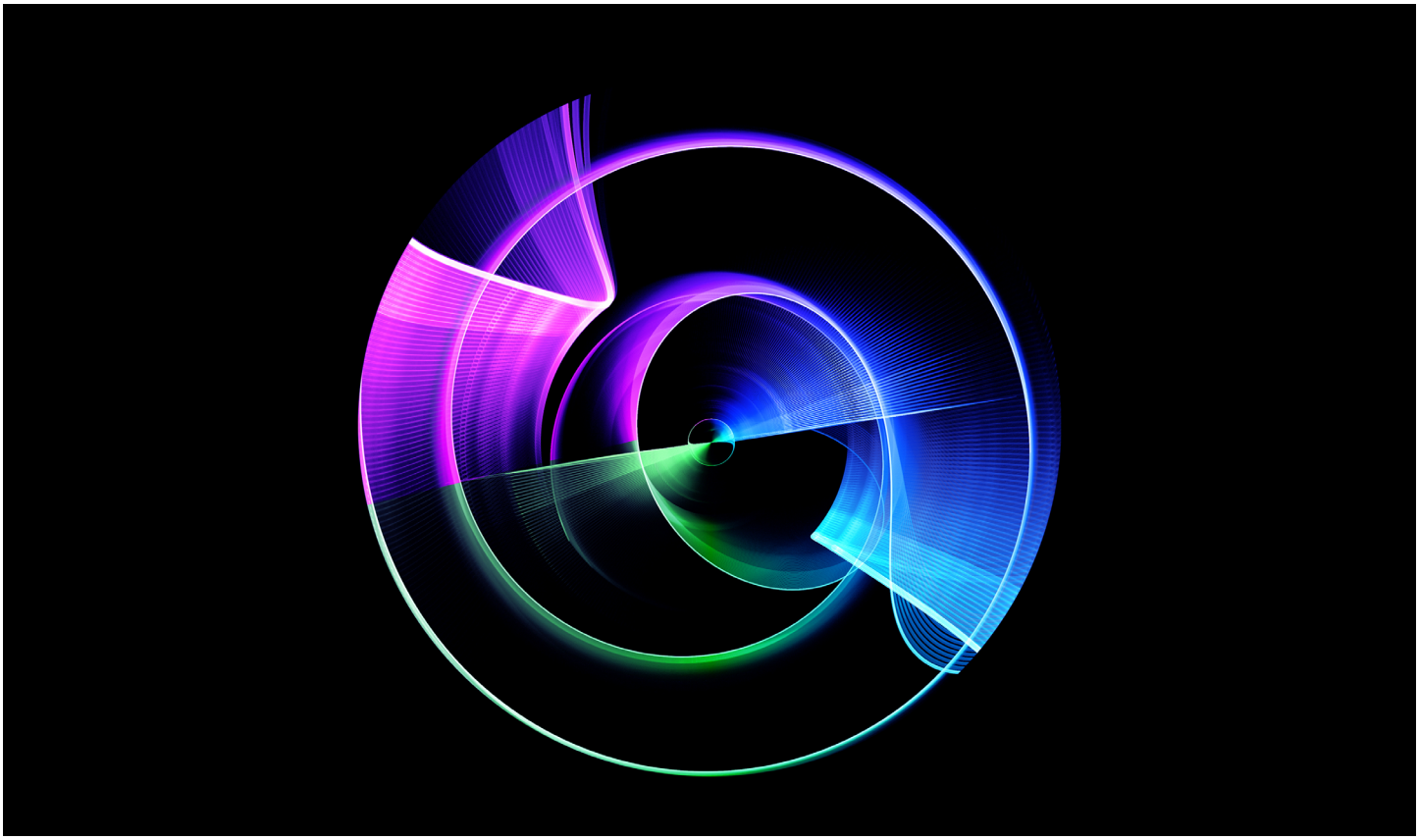
Deloitte.



AML risks in fintech alliances: Considerations for regional banks

It's easy to understand the appeal of fintech partnerships for financial institutions. Fintechs can offer a multitude of solutions, such as more modernized systems, new product offerings, and expansive customer bases, particularly for regional banks that may look to fintech partnerships as a strategic market opportunity for growth.[1] Nevertheless, the adoption of innovative fintech offerings may result in a more complex operating environment for the bank, potentially exposing it to new or heightened risk considerations. Specifically, fintech partnerships can pose money laundering risks that must be considered, and regulators are taking notice.

In September 2022, Blue Ridge Bank entered into an agreement with the Office of the Comptroller of the Currency (OCC) following concerns with its fintech partner's customer onboarding practices and material gaps in Blue Ridge's anti-money laundering (AML) compliance program.[2] As part of the agreement, Blue Ridge Bank agreed to bolster its AML program and seek OCC approval prior to engaging in any future fintech partnerships. While the implications of the agreement go beyond AML compliance, the scope of this article will focus on AML.

As the fintech industry has grown and bank-fintech alliances have become more frequent, so, too, has regulatory scrutiny of fintechs and their banking partners.

Risk considerations

In the past, fintechs were less constrained by regulations than established financial institutions. As the fintech industry has grown and bank-fintech alliances have become more frequent, so, too, has regulatory scrutiny of fintechs and their banking partners. Because fintech AML regulation is still a grey and nascent area, and banking regulations are more established, regulators are somewhat forced to focus on the banking partners that enable or leverage fintech products. It is therefore crucial for banks to understand and address the risks presented by a fintech partnership before any alliance is initiated. AML risk considerations that banks should assess include the following:

Know your (end) customer

In conducting due diligence on a potential fintech partnership, banks should not overlook the end user of the services that the bank and fintech will offer. As with the bank's preexisting customers, banks must know and assess who the fintech's customers are, from where their funds are sourced, and screen these customers against sanctions and politically exposed persons (PEP) lists. The fintech should have a customer risk rating model in place with enhanced due diligence procedures established for high-risk customers that is consistent with the bank's AML policy and risk appetite. Banks cannot simply assume that a fintech's policies, procedures, and operational practices are sufficient; the regulatory obligation to know and screen the customer remains with the bank.

Products and services

The products and services that the fintech offers, as well as those that the partnership will incorporate, can contribute to an increased AML risk exposure for the bank. Fintechs' product offerings vary widely from domestic banking and payments to international transfers and blockchain/cryptocurrency offerings such as digital wallets. The AML risk may increase with more complex, novel, or international offerings, and this should be accounted for in the risk assessment and partnership decision.

Monitoring

If the fintech is performing suspicious activity transaction monitoring on the bank's behalf, evaluation of the fintech's transaction monitoring program should be performed to understand if it meets the bank's standards, regulatory expectations, and industry practices. This assessment should cover transaction monitoring for AML, fraud, and sanctions screening, as well as the fintech's investigation life cycle for positive alerts, including investigation, escalation, and suspicious activity reporting. Each of these monitoring components should be assessed in conjunction with understanding the fintech's data practices. Banks should consider looking into the data quality, traceability, and transparency of a fintech's systems, as well as consider a stipulation that a fintech partner agrees to grant the bank access to full transactional data during the course of the alliance.

Contingency plans

The decision to enter into a fintech partnership is a strategic one, and a holistic contingency plan is needed from a strategic standpoint. If, for any reason, a fintech was unable to continue operating, the bank may be required to absorb the fintech's customers as its own. The bank must have a response plan in place for such situations, including whether additional infrastructure would be needed, whether data can readily be integrated, and whether the bank has the resources to handle the potential increase in volume and activity.

Compliance program

Fintechs should have a robust risk and compliance management program covering governance, risk assessment, AML and sanctions training, and monitoring, among others.[3] The bank must analyze these pillars to see if and how its own compliance program aligns with that of a potential partner and in what ways these programs will be able to work together to support one another. Overall, the objective should be to determine if a fintech has a compliance program and corresponding controls in place that are commensurate with the bank's risk appetite of regulatory obligations.

Toward a standardized approach

The recent growth in banking as a service (BaaS) and the resulting segmentation of a formerly concentrated banking industry has led to what the OCC has characterized as a blurred line "of where the bank stops and the fintech starts."[4] To address this, the OCC is working on a more nuanced approach to its oversight of bank-fintech partnerships, categorizing types of fintech alliances into cohorts broken down based on structure of the relationship and resulting risk profiles. This should help, in turn, to alleviate uncertainties and clarify expectations for each party involved in a partnership. Tailored guidance per category will then be issued, with which banks should assess and align their third-party compliance management programs with.

Nevertheless, a proactive approach in addressing fintech AML risk is warranted. The OCC has already urged financial institutions to assess their risk exposure and manage the impact of fintechs on their organizations.[5] Following the Blue Ridge Bank agreement, regulators will likely continue to scrutinize banks with similar fintech partnerships to determine whether these arrangements have the appropriate controls in place to address the unique AML risks posed by the relationship. With a thoughtful and thorough approach to fintech partnerships and the related AML risk management, the strategic goals of the alliance can be achieved without jeopardizing compliance standards.

Contacts

Michael Shepard
Principal, Deloitte Risk & Financial Advisory,
Forensic & Financial Crime
mshepard@deloitte.com

Carrie Meneo
Senior Consultant, Deloitte Risk & Financial Advisory,
Forensic & Financial Crime
cmeneo@deloitte.com

Endnotes

1. Deloitte, "Closing the gap in fintech collaboration", 2018
2. US Securities and Exchange Commission (SEC), "Exhibit 10.1: Agreement by and between Blue Ridge Bank, National Association, Martinsville, Virginia and the Office of the Comptroller of the Currency," accessed February 20, 2023.
3. Deloitte, "Fintech risk and compliance management", 2019
4. US Office of the Comptroller of the Currency (OCC), "Acting Comptroller of the Currency Michael J. Hsu remarks at the TCH + BPI Annual Conference 'Safeguarding Trust in Banking: An Update'," September 7, 2022.
5. OCC, Semiannual risk perspective from the National Risk Committee, spring 2022.

Deloitte.

About Deloitte

This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte shall not be responsible for any loss sustained by any person who relies on this publication.

As used in this document, "Deloitte" means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.