THE REVIEW OF
BANKING & FINANCIAL SERVICES
A PERIODIC REVIEW OF SPECIAL LEGAL DEVELOPMENTS AFFECTING LENDING AND OTHER FINANCIAL INSTITUTIONS

Vol. 40 No. 10 October 2024

FBO ACCOUNTS: MAXIMIZING BENEFITS WHILE MINIMIZING RISKS IN FINTECH PARTNERSHIPS

Innovation in the banking and fintech industry has been supported in many cases through "FBO" or "for the benefit of" accounts that are set up by banks and their fintech partners to move funds for customers. These accounts are popular with fintechs because of the potential to help them minimize money transmission licensing risk. Despite the popularity of the FBO account model, there are numerous legal and regulatory risks that banks and their fintech partners need to take into consideration. These risks and their management are discussed in this article.

By Andrew E. Bigart and Max Bonici *

Over the past decade, the fintech industry and its bank partners have been at the forefront of developing innovative financial services for consumers and businesses.[1] This innovation is reflected through the many buzzwords used to describe fintech services, such as BaaS, BNPL, and P2P, among many others. But there is perhaps one that stands out above all others: FBO account. The "FBO" or "for the benefit of" account has become the engine that drives fintech services, from payments to lending and other activities that involve the movement of funds on behalf of customers.

At the most basic level, an FBO account is a custodial deposit account established by a bank partner of a non-bank fintech for purposes of receiving, managing, and transmitting funds "for the benefit" of the fintech's customers. The FBO account has become a critical tool that fintechs have leveraged to minimize the risk of triggering federal and state money transmission registration and licensing requirements when providing financial services (especially in the absence of a feasible federal fintech charter/license).

Despite the ubiquity of FBO accounts, there are numerous legal and regulatory risks that banks and their fintech partners need to take into consideration. In particular, the failure of three U.S. regional banks in the spring of 2023 set off a trend of heightened regulatory, supervisory, and enforcement activity among the federal banking agencies.[2] This scrutiny has extended to bank–fintech partnerships, including the use of FBO accounts.

[1] In this article, we generally refer to any insured depository institution as a "bank."

[2] The term "federal banking agencies" refers to the Federal Deposit Insurance Corporation ("FDIC"), the Board of Governors of the Federal Reserve System (the "Federal Reserve"), and the Office of the Comptroller of the Currency ("OCC").

*ANDREW E. BIGART is a partner and MAX BONICI is a counsel in the Financial Services practice of Venable LLP in the Washington, DC office. Their e-mail addresses are aebigart@Venable.com and mbonici@Venable.com.

RSCR Publications LLC Published 12 times a year by RSCR Publications LLC. Executive and Editorial Offices, 2628 Broadway, Suite 29A, New York, NY 10025-5055. Subscription rates: $650 per year in U.S., Canada, and Mexico; $695 elsewhere (air mail delivered). A 15% discount is available for qualified academic libraries and full-time teachers. For subscription information and customer service call 609-683-4450; fax 609-683-7291; write Subscriber Services, RSCR Publications, PO Box 585, Kingston NJ 08528; e-mail cri.customer.service@comcast.net; or visit our website at www.rscrpubs.com. General Editor: Michael O. Finkelstein; tel. 212-876-1715; e-mail mofinkelstein@gmail.com. Associate Editor: Sarah Strauss Himmelfarb; tel. 301-294-6233; e-mail sarah.s.himmelfarb@gmail.com. To submit a manuscript for publication contact Ms. Himmelfarb. ISSN: 1051-1741.

The recent bankruptcy of Synapse, a leading fintech that purportedly lost millions of dollars of customer funds held in FBO accounts, may draw additional regulatory focus on this business model and raise questions about potential gaps in the regulatory framework.

As explained in this article, any bank that provides FBO account services for fintechs should prepare for heightened regulatory scrutiny in areas including anti-money laundering ("AML") compliance, safety and soundness, account ledgering, and customer payment reconciliation, FDIC deposit insurance, and consumer financial protection. Fintechs should take a close look at their bank partnerships to ensure that the FBO accounts are structured to provide the best defense against claims of unlicensed money transmission or similar state-licensed activity. While the focus below is on some of the challenges associated with the FBO model, the discussion should not be taken as suggesting that the model lacks merit, but rather as a reminder that as banks and fintechs continue to innovate, they should keep in mind that the regulators are watching (as expected) to make sure that safety and soundness, consumer protection, and other important issues are not left behind.

WHAT IS AN FBO ACCOUNT?

An FBO account typically is a deposit account opened by an insured depository institution (e.g., as custodian) to receive, hold, and transmit funds on behalf of one or more other parties (the "beneficiaries"). In a typical bank–fintech partnership, the bank that opens and manages the account will hold legal title to it and describe it along the lines of "FBO [FINTECH] Customers." The beneficiaries are the individuals or entities that benefit from the funds or assets in the account. Although the beneficiaries do not have direct control over the account, they have an interest in the assets held in it.

The flow of funds through the account is managed pursuant to the contract between the bank and the fintech. This agreement will typically set forth the fintech's right to provide payment instructions to the bank to move funds in and out of the account. At the same time, the fintech executes a separate agreement with each beneficiary that determines how the fintech will use the funds for the beneficiary — for instance, to pay another party, or to transfer the money to another account of the beneficiary, among other options.

Under FDIC rules, provided adequate recordkeeping and other requirements are satisfied, FBO arrangements allow each beneficiary to receive pass-through FDIC deposit insurance. As a result, even though there is only one deposit account, each beneficiary's funds are insured up to the applicable maximum deposit insurance limit, for instance, $250,000 for a single individual or entity, or $500,000 for joint accounts (e.g., for spouses), among other options and combinations.

HOW ARE FBO ACCOUNTS USED TO POWER PAYMENTS AND FINTECH?

By using an FBO account, fintechs and other entities looking to provide payments-related services to customers can rely on a partner bank to handle many of the regulated activities without the need for the non-bank entity to be licensed. There is a reasonable argument that a fintech that provides payment instructions to a bank to move funds through a properly structured FBO account does not engage in money transmission under federal and state laws.

Money transmission in the United States is regulated at the federal and state levels. At the federal level, money transmitters are regulated under the Bank Secrecy Act ("BSA").[3] The Financial Crimes Enforcement Network ("FinCEN"), part of the U.S. Treasury Department, administers the AML regulations implementing the BSA and has established registration and AML program requirements for money transmitters.[4] In addition, 49 states and the District of Columbia require money transmitters to obtain a license from the state's financial regulator.

Since federal and state law definitions of money transmission typically require the "receipt" and "transmission" of funds, there is a reasonable and

[3] 31 U.S.C. 5311 *et seq*.

[4] 31 C.F.R. Ch. X. The AML program requirements include implementation of policies and procedures for performing customer due diligence and monitoring and reporting on suspicious transactions, among various other requirements.

straightforward case to be made that a fintech does not engage in money transmission (e.g., does not receive and transmit funds) where all funds pass through a bank-owned and controlled FBO account. While there is limited guidance in this area, there are several federal and state money transmission advisory opinions and state court decisions that support this conclusion.[5]

For this reason, FBO-type accounts are used by fintechs to facilitate payments in a number of use cases, including:

- *P2P Payments*. Fintech platforms use FBO accounts to manage transfers between users.
- *Merchant Payments*. Payment processors hold merchant funds in FBO accounts. When a customer makes a payment, the funds are held in an FBO account until they are transferred to the merchant's bank account.
- *Digital Wallets*. Fintechs use FBO accounts to manage user balances. Users deposit funds into their digital wallets, which are held in FBO accounts until they are spent or withdrawn.
- *Subscription Services*. Fintech companies that manage recurring payments use FBO accounts to handle transactions efficiently.
- *Peer-to-Peer Lending Platforms***.** These entities use FBO accounts to collect funds from investors and disburse them to borrowers.
- *Investment Platforms*. So-called robo-advisors and other investment services manage client investments through FBO accounts, ensuring proper allocation and security of funds.

In addition to providing a potential solution to a fintech's money transmission challenge, FBO accounts present certain other benefits. The accounts allow fintechs to segregate customer funds from the fintech's operational funds. This may be required under certain state licensing frameworks. When done properly, it can help ensure that customer funds are protected even if the fintech faces financial difficulties. Thus, FBO accounts simplify the management of funds for multiple users. Instead of creating an individual account for each user, fintechs can leverage streamlined accounting and reconciliation processes, reducing administrative overhead and cost, and providing additional speed.

While FBO accounts are typically managed through individual sub-accounts for the beneficiaries, more recent models have included the use of "virtual accounts" to track payments for individual beneficiaries. All of this, of course, assumes that the bank or fintech has appropriate controls in place to track and reconcile funds movements — an assumption, as discussed in greater detail below, that may not always be accurate.

Finally, the accounts can be interest-bearing, which may benefit both fintech companies and their customers, although this is another area in which there is limited guidance, suggesting that banks and fintechs should proceed cautiously. On the one hand, banks may pay interest on these accounts, providing fintech companies with additional revenue or the ability to offer interest to their users or, in some models, allowing fintechs to offer higher interest rates than customers might otherwise receive. On the other hand, if the fintech receives interest from the accounts it may undermine arguments that the fintech does not own or control the account from a money transmission perspective. In practice, our experience has been that most arrangements do not involve the payment of interest.

WHAT ARE SOME OF THE KEY LEGAL CONSIDERATIONS WITH FBO ACCOUNTS?

The use of FBO accounts generally, and within the bank–fintech partnership context specifically, is rife with supervisory, regulatory, and enforcement scrutiny, and, as a result, both banks and fintechs involved with FBO accounts should carefully consider a number of legal considerations. As noted above, if it is structured properly, there are good arguments that an FBO arrangement insulates the participating fintech from money transmission risk. Accordingly, in the discussion below, we focus on federal legal requirements relevant to FBO accounts, principally those in statute and regulation, as well as the sub-regulatory guidance that agencies have developed to explain these authorities,rather than state issues associated with money

[5] *See, e.g.*, FinCEN, Application of Money Services Business Regulations to a Company Acting as an Independent Sales Organization and Payment Processor, FIN-2014-R009 (Aug. 27, 2014) (explaining that an entity that "neither accepts nor transmits funds on behalf of the merchants . . ., nor on behalf of the . . . counterparties" does not engage in money transmission); *Pincus v. Speedpay, Inc.*, 741 Fed. Appx. 720, 722 (11 Cir. 2018) ("An essential prerequisite to being a 'money transmitter' is that the corporation 'receives' currency for the purpose of transmitting the same.").

transmission licensing.[6] In particular, at the federal level, the banking agencies issued a joint statement in July 2024 outlining potential risks in bank-fintech arrangements along with a request for public comment.[7] Together, the documents address many of the risks noted herein, and recognize the important role that FBO accounts have played in the growth of the bank-fintech partnership model.

1. Anti-Money Laundering and Counter-Terrorist Financing

The BSA[8] and FinCEN regulations require banks[9] (among other obligations) to establish written AML programs that include customer identification ("CIP") and customer due diligence ("CDD") programs for each "customer" that opens an "account."[10] There is little federal guidance, however, that addresses how banks should treat FBO accounts from a CIP and CDD perspective.

Under FinCEN regulations, an "account" is defined as a formal banking relationship to provide or engage in services, dealings, or other financial transactions, and includes a deposit account and other transaction or asset accounts, among others.[11] An account also includes a relationship established to provide a safety deposit box or other safekeeping services, or to provide cash management, custodian, or trust services.[12] An account does not include products or services for which a formal banking relationship is not established with a person, such as check cashing, wire transfer, or the sale of a check or money order,[13] or in instances when an application for deposit or other banking services is denied.[14]

In general, a bank is not required to "look through" its customer relationship to apply its CIP and CID programs to its customer's customer, including with respect to "parties having rights against the entity opening a pooled account for purposes of payment processing."[15] Similarly, FinCEN has advised that a "bank will not be required to look through trust, escrow, *or similar accounts* to verify the identities of beneficiaries and instead will only be required to verify the identity of the named accountholder."[16]

Notwithstanding this general guidance, the federal banking agencies and FinCEN have explained that "in certain situations, banks should 'look through' pooled accounts to identify an individual or entity utilizing the account as a customer for purposes of CIP," especially where the individual or entity using the account has established a formal agreement with the bank in connection with accessing the account.[17] Similarly, the federal banking agencies have issued guidance concluding that a bank was required to perform CIP on general-purpose open-loop prepaid cardholders where the cardholders had "(1) the ability to reload funds or (2) access to credit or overdraft features."[18] According to the guidance, these types of activities constitute the establishment of a formal banking relationship, presumably because the bank is providing the cardholder

[6] State statutes, regulations, and guidance may also bear on some of these considerations but are not discussed in this article.

[7] Request for Information on Bank-Fintech Arrangements Involving Banking Products and Services Distributed to Consumers and Businesses, 89 F.R. 61577 (July 31, 2024).

[8] 31 U.S.C. §§ 5311 *et seq*.

[9] 31 C.F.R. Chapter X. Various AML obligations and prohibitions may apply to other financial institutions, as defined under the BSA and FinCEN regulations. This article generally discusses banks as insured depository institutions.

[10] 31 C.F.R. § 1020.220.

[11] 31 C.F.R. § 1020.100(a)(1).

[12] *Id.*

[13] 31 C.F.R. § 1020.100(a)(2)(i), (ii).

[14] Customer Identification Programs for Banks, Savings Associations, Credit Unions, and Certain Non-Federally Regulated Banks, 68 Fed. Reg. 25090, 25093 (May 9, 2003) (Joint Final Rule).

[15] *See, e.g.*, OCC Interpretive Letter 1175, (December 2020).

[16] FIN. CRIMES ENF'T NETWORK, INTERAGENCY INTERPRETIVE GUIDANCE ON CUSTOMER IDENTIFICATION PROGRAM REQUIREMENTS UNDER SECTION 326 OF THE USA PATRIOT ACT (2005);68 Fed. Reg. 25090, 25094 (May 9, 2003).

[17] OCC Interpretive Letter 1175, (December 2020) (explaining that where a bank provided services to software providers and their merchants in connection with processing customer payments through a pooled FBO account, the bank was required to perform CIP on the software providers and the merchants because they (1) were using the custodial account to process payments for their sales and related activities and (2) had established formal agreements with the bank in connection with these merchant processing activities. This was the case even though the software platform and merchants were not the named holders of the FBO account).

[18] *Id*.

with direct access and control over the funds held in the pooled account established for the prepaid card program.

Accordingly, the extent to which a bank may have CIP or CDD obligations with respect to the beneficiaries of an FBO account will depend on the facts and circumstances, particularly the extent to which the beneficiaries may have direct agreements with the bank or otherwise have the ability to directly control or access the FBO account. This means that each FBO arrangement should be reviewed to ascertain the CIP and/or CDD implications and the associated responsibilities of the bank and the fintech.

Notwithstanding the above discussion, banks may impose on fintech partners certain diligence and notification requirements by contract, as part of the bank's AML/CFT programs, depending on the bank's own risk appetite and determinations. In these cases, AML obligations may be passed on to fintech partners, even if the fintech does not meet the definition of "financial institution" under the BSA and FinCEN regulations[19] and does not otherwise have direct AML obligations under federal law. At a minimum, regulators will expect the financial institution to ensure that its fintech partners have robust AML programs in place that are consistent with both applicable law and the bank's internal policies and procedures.

2. Third-Party Risk Management

The FDIC, Federal Reserve, and OCC 2023 interagency guidance on Third-Party Risk Management ("TPRM") (the "TPRM Guidance") outlines key elements and expectations for banks to manage risks associated with third-party relationships, which include products and services they provide or receive via contract or otherwise. The key stages of the TPRM life cycle are (1) planning, (2) due diligence, (3) contract negation, (4) ongoing monitoring, (5) risk management, and (6) termination.

The TPRM Guidance is especially relevant to bank–fintech partnerships and FBO arrangements and remains an important policy focus for the federal banking agencies, in both supervision and enforcement. For instance, the FDIC released a consent order in January 2024 that requires a bank to offboard some of its fintech partners, among other notable requirements.[20] According to the order, the enforcement action stemmed from management issues in connection with the bank's use of FBO accounts, among other factors. Under the consent order, the bank and all fintechs involved are heavily limited or scrutinized:

- TPRM-related requirements are imposed on all fintechs with which the bank has a relationship — both third-party fintechs and fintechs with which the bank has a direct relationship.
- The bank must retain a third party to review its TPRM program and conduct the due diligence expected under the TPRM Guidance.
- The bank must limit the annual growth of assets and liabilities to under 10%, terminate "significant" fintech partnerships, and increase its Tier 1 regulatory capital.
- Much of the bank's TPRM program, including onboarding for new fintech partners, is subject to the review and comment of the FDIC regional director for the bank.

Banks looking to leverage third-party relationships such as fintech partnerships that involve FBO arrangements must carefully navigate the TPRM Guidance and the evolving expectations of the federal banking agencies, which are currently being clarified in supervision and public enforcement actions. While under the TPRM Guidance, the contract negotiation stage of the TPRM life cycle would appear to have received the most focus of the federal banking agencies (as described), in practice, the ongoing monitoring requirement has emerged in public enforcement actions as an area of agency focus. It is also important that banks and fintechs understand that termination is not a mere suggestion or possibility; it is an expectation under the TPRM Guidance, and if banks do not terminate fintech partners as required, the federal banking agencies may direct banks to do so in supervision or enforcement.

3. Safety and Soundness

Section 39 of the Federal Deposit Insurance Act (the "FDI Act")[21] requires the federal banking agencies to

[19] *See generally* 31 U.S.C. § 5312(a)(2); 31 C.F.R. § 1010.100(t).

[20] In the Matter of Lineage Bank, Franklin, Tennessee, FDIC, Consent Order FDIC-23-0041b (January 30, 2024), https://orders.fdic.gov/sfc/servlet.shepherd/document/download/0693d00000BrElHAAV?operationContext=S1.

[21] *See, e.g.*, 12 U.S.C. § 1831p–1 (Standards for safety and soundness); 12 C.F.R. pt. 30 and App'x A (OCC), pt. 208 and App'x D-1 (Federal Reserve), pt. 364 and App'x A (FDIC).

footnote continued from previous column…

establish operational and managerial standards to promote the general safety and soundness of banks. While these standards are broad, bank–fintech relationships, the accounts derived from them — including those involving FBO arrangements — and the assets and liabilities associated with these accounts and any attendant risks, including concentration risk, are covered by this general safety and soundness provision. Banks therefore must carefully consider FBO relationships in line with their general risk framework.

In particular, one area that may require consideration is whether the FBO account arrangement raises any issues under the FDIC's rules governing deposit brokers and brokered deposits.[22] Section 29 of the FDI Act restricts banks that are less than well-capitalized from accepting brokered deposits[23]; however, adequately capitalized banks may request a waiver from the FDIC to accept brokered deposits.[24] Depending on the specific facts of the FBO arrangement, the fintech could potentially meet the definition of deposit broker by (1) engaging in the business of placing deposits of third parties with banks or (2) engaging in the business of facilitating the placement of deposits of third parties with banks. Nevertheless, it is ultimately the bank that has the compliance obligation and must determine whether a deposit is a brokered deposit and whether it may accept it.

4. Account Ledgering, FDIC Deposit Insurance, and Related Considerations

As a practical matter, the bank and fintech offering the FBO services will need accurate and reliable ledgering, and reconciliation processes to track funds that flow into and out of the account. While the need for accurate records may seem an inherent component in providing financial services, the recent collapse of Synapse, one of the largest users of FBO accounts, demonstrates that maintaining procedures to manage funds movement can be difficult in practice.

In many cases, the bank may require its fintech client to maintain the ledger record of funds held in an FBO account, while maintaining monitoring and oversight rights and responsibilities. It is also increasingly common for a bank to assign the various "beneficiaries" virtual accounts for purposes of tracking funds and amounts owed. A virtual account is a reference and/or other unique identifier that can be used to track the transfer of funds into and out of the FBO account.[25] Take, for example, a fintech that offers a bill payment solution for businesses. Each of the fintech's customers can direct the fintech to send funds through the FBO account to dozens of suppliers and other payees. If the fintech achieves scale, it could find itself needing to track a significant number of transactions for numerous customers moving through the FBO account each day.

In practice, the fintech will need to implement sophisticated ledgering and reporting technology. And, from the bank's perspective, even if the fintech is assigned the ledgering responsibilities, the bank may not be able to avoid potential liability and operational headaches if something goes wrong. The movement of funds is a core function of FBO arrangements, and the failure to track and manage the funds can result in customer inconvenience (at best) and losses (at worst). These challenges are magnified when the fintech manages programs for various sub-fintechs. In these cases, banks will often require a separate FBO account for each of the sub-fintechs and/or programs being offered.

With respect to Synapse, for example, several of the fintech's bank partners are wrapped up in the bankruptcy proceeding and working with the appointed bankruptcy trustee to recover and distribute customer funds. The bankruptcy has already drawn the attention of Congress, and the potential loss of customer funds will undoubtedly be looked at closely by the federal banking agencies.

With respect to the potential loss of customer funds, the FDIC insures eligible funds up to the standard maximum deposit insurance amount: $250,000 per depositor, per insured bank, for each account ownership category.[26] Often the addition of "FBO" to an account name is part of the recordkeeping process for determining the parties that benefit from FDIC deposit

[22] 12 C.F.R. § 337.6 (brokered deposits) (a provision of Part 337 (Unsafe and Unsound Banking Practices)).

[23] 12 U.S.C. §§ 1813f(a), (c).

[24] Thus, although filings with the FDIC may be required for certain deposit brokers, the FDIC does not license deposit brokers.

[25] Virtual accounts are not bank accounts (or sub-accounts), but rather unique identifiers used for ledgering purposes within a master account. Virtual accounts provide a tool for the segregation of data, balance analysis, and transaction identification similar to what would be used in connection with a traditional sub-account.

[26] Deposit insurance is calculated, dollar for dollar, based on the principal plus any interest accrued or due to the depositor, through the date of default.

insurance coverage, particularly on a pass-through basis. Terms such as "FBO," "in custody for," or "in trust for" are intended to indicate an agency relationship between the party that opened the account or deposited the funds and the parties that actually own the funds. When there is a dispute over ownership of an account, courts generally look to the totality of the circumstances to determine the owner of the funds. While the decision of how to name an account is viewed as an indicator of the parties' intentions, courts typically focus on the conduct of the parties and any agreements between them to determine ownership.

Under the FDI Act and FDIC regulations, if an FBO account is structured to meet applicable FDIC regulations for pass-through insurance, FDIC deposit insurance is available to each depositor (individual or entity[27]) that has funds within the FBO account up to the maximum deposit insurance amount. Specifically, the members would likely qualify for FDIC pass-through insurance if:[28]

- The funds are held in a trust, agency, nominee, or custodial account;
- The fiduciary relationship is disclosed in the account records (e.g., the account is titled "FBO [FINTECH NAME]'s Members";
- The name of each principal is ascertainable from either the bank's records or the records of the agent/fiduciary in whose name the account is titled (e.g., the fintech maintains accurate sub-account ledgers for each member); and
- The amount owed to each principal is "known at that time [of default]" and may be determined "on a fractional or percentage basis."

Another important consideration is the prohibition in Section 18(a)(4) of the FDI Act against making any false or misleading representations about deposit insurance, using the FDIC's name or logo in a manner that would imply that an uninsured financial product is insured or guaranteed by the FDIC, or knowingly misrepresenting the extent or manner of deposit insurance.[29] Under the FDIC's regulations, a statement regarding deposit insurance violates the FDIC's regulations if the statement (1) contains any material representations that would have the tendency or capacity to mislead a reasonable consumer or (2) omits material information that would be necessary to prevent a reasonable consumer from being misled.[30] A consumer does not actually have to be misled for a statement to be deemed misleading under the FDIC's regulations.[31]

The FDIC has the authority to investigate violations of the advertising and marketing rules under the FDI Act and Part 328.[32] These include cease and desist letters against non-bank parties and partners of banks, as well as other actions. Since 2022, the FDIC has sent several such letters to fintechs advising them to cease and desist making false and misleading statements about FDIC deposit insurance coverage.[33] The FDIC also maintains a public database of persons who have made such false or misleading representations.[34]

5. Consumer Financial Protection

A final area of risk worth highlighting is the potential for a bank–fintech partnership to raise consumer protection risks. These concerns extend beyond the use of an FBO account and touch upon the broader bank–fintech partnership, including the provision of the underlying financial service. On this point, there is no shortage of federal and state regulatory authorities

[27] Referred to as "principals" under the FDIC's regulations. 12 C.F.R. § 330.7(a).

[28] 12 U.S.C. §§ 1813(m) ("insured deposit" means "the net amount due to *any* depositor for deposits in an insured depository institution as determined under sections 7(i) and 11(a)") (emphasis added), 1813(*l*)(3); 12 C.F.R. §§ 330.3(i)(1), 330.5(a)(2) and (b), 330.7(a). The FDIC has discretion to determine whether the evidence of deposit ownership and recognition of such ownership in custodial accounts is satisfactory.

[29] 12 U.S.C. § 1828(a)(4).

[30] 12 C.F.R. § 328.102(b)(3).

[31] *Id*.

[32] 12 C.F.R. §§ 328.106 (informal resolution authority), 328.107 (formal enforcement powers).

[33] *See, e.g.*, FDIC Demands Five Entities Cease Making False or Misleading Representations about Deposit Insurance, FDIC (January 19, 2024), https://www.fdic.gov/news/press-releases/2024/pr24003.html; FDIC Demands Three Companies Cease Making False or Misleading Representations about Deposit Insurance, FDIC (June 15, 2023), https://www.fdic.gov/news/press-releases/2023/pr23049.html.

[34] Database on the *Prohibition under Section 18(a)(4) of the Federal Deposit Insurance (FDI) Act*, https://www.fdic.gov/resources/regulations/laws/section-18a4-of-fdi-act/index.html#:~:text=Insurance%20(FDI)%20Act-,Section%2018(a)(4)%20of%20the%20Federal%20Deposit%20Insurance,by%20the%20FDIC%2C%20or%20knowingly.

keeping a watchful eye on bank–fintech partnerships, including for potential violations of unfair or deceptive acts and practices.

- The Federal Trade Commission ("FTC") has broad investigative and enforcement powers under Section 5 of the Federal Trade Commission Act (the "FTC Act"), which prohibits unfair or deceptive acts or practices.[35] While the FTC does not have jurisdiction over banks, the federal banking agencies have authority to enforce Section 5 of the FTC Act for the institutions they supervise and their institution-affiliated parties.[36] Unlike many other consumer protection laws, Section 5 of the FTC Act may extend in certain cases to transactions that impact business customers as well as individual consumers.[37]

- The federal banking agencies have authority under Section 8 of the FDI Act to issue enforcement actions or take other measures when a UDAP violation is cited.[38] The FTC has authority to take action against non-banks that engage in an FTC UDAP. If a UDAP involves an entity or entities over which more than one agency has enforcement authority, such as, for example, the FDIC and the FTC, the agencies may coordinate their enforcement actions.[39]

- The CFPB has supervisory jurisdiction specifically over banks with total assets in excess of $10 billion, as well as any other "covered person" or "service provider" under the Consumer Financial Protection Act.[40]

- The Securities and Exchange Commission and the Financial Industry Regulatory Authority have authority to monitor advertising and marketing practices in the securities and broker–dealer industries.

These regulators are likely to focus on many of the issues discussed, including AML compliance, safety and soundness, and management of customer funds (as applicable). But they will also focus on broader advertising and marketing practices. While most fintechs do not advertise the use of FBO accounts directly, they are likely to market the overarching financial service through social media, online, and other media. In connection with such marketing, fintechs and their bank partners must avoid misleading claims related to the pricing or performance of a product or service, deceptive endorsements or fake reviews, or other "dark patterns." Most recently, regulators have challenged various fee practices as "junk fees" that bear little relation to the cost of providing the service or that are not clearly disclosed and explained.

Thus, even if an FOB arrangement is structured carefully to address AML, safety and soundness, and other risks, there are still pitfalls that can create unexpected challenges. A bank looking to provide FBO services to a fintech must take all of these issues into account, in addition to the more traditional banking considerations discussed throughout this article.

CONCLUSION

Working together, banks and fintechs have brought various new and innovative financial products and services to market. These services have increased competition and expanded access to financial services. Many of these services are supported through FBO and other, similar pooled accounts. And while these models offer numerous benefits, they also raise various legal and regulatory considerations. Any bank or fintech considering a program that involves the use of an FBO account should take care to structure the arrangement carefully from the outset, to minimize the risk of regulatory headaches down the road. ■

---

[35] 15 U.S.C. § 45.

[36] FDIC, CONSUMER COMPLIANCE MANUAL, VII-1.2. (2022) (Unfair, Deceptive, and Abusive Practices — Federal Trade Commission Act/Dodd-Frank Act).

[37] *Id.*

[38] 12 U.S.C. § 1818.

[39] FDIC, CONSUMER COMPLIANCE MANUAL, VII-1.2. (2022) (Unfair, Deceptive, and Abusive Practices - Federal Trade Commission Act/Dodd-Frank Act).

[40] 12 U.S.C. §§ 5515(a)(1) (banks), 1024 (supervision of nondepository covered person).