AMERICAN BANKERS ASSOCIATION, KRISTA SHONK

Proposal and Comment Information

Title: Request for Information on Bank-Fintech Arrangements Involving Banking Products and Services Distributed to Consumers and Businesses , OP-1836

Comment ID: FR-0000-0134-01-C135

Submitter Information

Organization Name: American Bankers Association

Organization Type: Organization

Name: Krista Shonk

Submitted Date: 10/30/2024

Krista Shonk
SVP & Sr. Counsel
Fair and Responsible Banking
kshonk@aba.com

October 30, 2024

James P. Sheesley
Assistant Executive Secretary
Federal Deposit Insurance Corporation
550 17th Street NW Washington, DC 20429
Attention: Comments RIN 3064-ZA43

Chief Counsel's Office
Office of the Comptroller of the Currency
400 7th Street SW Suite 3E–218
Washington, DC 20219
Attention: Comment Processing, Docket ID OCC 2024-0014

Ann E. Misback
Secretary
Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue NW
Washington, DC 20551
Attention: Comments Docket No. OP-1836

RE: Request for Information on Bank-Fintech Arrangements Involving Banking Products and Services Distributed to Consumers and Businesses

To Whom It May Concern:

The American Bankers Association[1] is pleased to comment on the Request for Information (RFI) on Bank-Fintech Arrangements Involving Banking Products and Services Distributed to Consumers and Businesses that was issued by the Board of Governors of the Federal Reserve System (Federal Reserve), the Federal Deposit Insurance Corporation (FDIC), and the Office of the Comptroller of the Currency (OCC). [2] The RFI solicits input on the nature of bank-fintech partnerships, effective risk management practices pertaining to these arrangements, and other implications of such partnerships.

The financial sector is melding banking and technology in new ways as the world economy undergoes a digital transformation. As this evolution unfolds, the RFI will be an important tool to help the agencies learn more about how banks partner with fintechs to deploy financial products and services. We urge the agencies to leverage the input generated by the RFI to modernize their approach to regulation and supervision and to provide banks with a meaningful, transparent, and consistent path to innovation. We appreciate the use of an RFI and encourage the agencies to continue to seek input from banks and other stakeholders as technology and bank partnerships evolve.

---

[1] The American Bankers Association is the voice of the nation's $23.9 trillion banking industry, which is composed of small, regional and large banks that together employ approximately 2.1 million people, safeguard $18.8 trillion in deposits and extend $12.5 trillion in loans.
[2] 89 Fed. Reg. 61578 (July 31, 2024).

Similarly, we recommend that the agencies jointly and holistically consider comments on this RFI, together with comments on related FDIC initiatives, to ensure that regulatory requirements do not duplicate existing laws or regulations and that supervisory practices are aligned, thereby avoiding regulatory arbitrage. It would not be prudent for just one agency to establish parameters around fintech activities or to identify areas of unmitigated risk.

Summary of the Comment

Banks are essential to the U.S. economy. They provide a secure way for individuals and businesses to store money; they facilitate commerce by processing payments; and they create economic opportunity by providing loans to consumers and businesses of all sizes. Banks are also intensely regulated and supervised. They are subject to an extensive framework of prudential laws and regulations to ensure that they operate in a safe and sound manner. And, they must comply with a wide range of consumer protection requirements intended to safeguard customer data, protect against fraud, ensure fairness and transparency, and prevent discrimination.

To remain competitive, banks often leverage technology to respond to customer demands for efficient delivery channels and seamless interfaces. Banks that do not innovate risk losing market share or becoming obsolete. In addition, innovation is central to achieving economies of scale to offset regulatory burden and cost pressures that are borne by banks of all sizes—and that pose a particular challenge to the community bank model.

Banks and fintechs play different—yet important—roles in the delivery of financial products and services. Banks have in-depth knowledge of laws and regulations; they are expert risk managers; they are also a source of trust and economic strength. In many cases, however, building new technology is outside of the core competencies of individual banks and their employees. Some banks have expanded their technological capability by partnering with fintechs.

As banks pursue strategies to serve customers in the digital economy, it is important that regulations keep up with rapid technological changes. The agencies should draft rules and policies to support responsible innovation and affirm well-managed bank-fintech partnerships. We provide several recommendations in this regard, including that the agencies:

- Consider comments on overlapping RFIs and proposed rules on an interagency basis to develop a consistent regulatory and supervisory approach to bank-fintech partnerships;
- Avoid generically labeling as "fintech" all third-party relationships that involve technology;
- Engage in meaningful, development-stage dialogue with banks and their fintech partners;
- Examine partner banks based on the structure of the fintech arrangement and the risks presented;
- Proactively share information with banks and fintechs regarding examination trends and regulatory concerns;
- Continue to enhance agency expertise on fintech-related topics;
- Conduct external education and outreach; and

- Conduct risk-based examinations of fintechs pursuant to the Bank Service Company Act.

We also emphasize that bank-fintech arrangements are not one-size-fits-all. They involve a wide range of products, structures, and practices, including variations on the degree to which the bank has a relationship with the end user, the allocation of responsibilities among the parties, the types of risk mitigants and controls the bank puts in place, the contractual terms that govern the relationship, and the extent to which the fintech is regulated or licensed at the state or federal level. We also note that not all bank relationships with fintechs are partnerships, and that some relationships with fintechs may be more appropriately characterized as customer relationships or vendor relationships, which represent a lower level of integration. For purposes of this comment letter, we focus mainly on partnerships. These characteristics have changed over the years and will continue to evolve.

We urge regulators to avoid viewing all bank-fintech partnerships as inherently risky and warranting heightened regulatory scrutiny, otherwise creating a stigma. Treating all arrangements as if they pose the same types and degree of risk is an inefficient use of regulatory resources, and would discourage the development of new products and delivery channels that enable banks to remain relevant and viable in the modern economy. It would also harm the customer experience. A regulatory posture that is perceived to be anti-innovation could be one factor that contributes to further bank consolidation, particularly in the community bank sector.

Finally, we appreciate that both the RFI and the simultaneously-published Joint Statement on Banks' Arrangements with Third Parties to Deliver Bank Deposit Products and Services (Joint Statement) identify potential risks posed by bank-fintech partnerships.[3] We provide additional information and commentary on a select number of these risks.

I. Regulators Should Support Responsible Innovation

A. The Agencies Should Consider Comments on Overlapping RFIs and NPRs Holistically

The RFI is part of a suite of regulatory initiatives that are designed to gather information to help the agencies formulate a policy approach to bank-fintech partnerships. It comes after a marked increase in enforcement actions against partner banks for inadequate third-party risk management practices and on the heels of the bankruptcy of Synapse Financial Technologies, Inc., which facilitated deposit relationships between fintechs and insured depository institutions.

These interrelated regulatory initiatives include:

- The Joint Statement on Banks' Arrangements with Third Parties to Deliver Bank Deposit Products and Services, which describes the risks and the risk management techniques that the agencies have observed in connection with deposit-generating bank-fintech partnerships;
- A Request for Information issued by the FDIC on the characteristics that affect the stability and franchise value of different types of deposits;[4]

---

[3] See https://www.occ.treas.gov/news-issuances/bulletins/2024/bulletin-2024-20.html.

[4] 89 Fed. Reg. 63946 (August 6, 2024).

- Proposed revisions to the FDIC's brokered deposit regulation that would significantly alter the economics and supervisory tolerance of bank-fintech partnerships, if not dissuade them altogether;[5] and
- A proposed rulemaking purportedly in response to the Synapse bankruptcy that would impose new recordkeeping requirements on "custodial deposit accounts with transactional features" that are held by insured depository institutions.[6]

We urge the agencies to consider comments on these proposals in a holistic manner to avoid an inconsistent or fragmented approach to bank-fintech partnerships. Considering the comments holistically will also increase the agencies' understanding of the issues presented. A coordinated effort will help to ensure that regulatory requirements do not duplicate existing laws or regulations and that supervisory practices are aligned, thereby avoiding regulatory arbitrage. It would not be prudent for just one agency to establish parameters around fintech activities or to identify areas of unmitigated risk.

B. The Agencies Should Avoid Generically Labeling as "Fintech" All Third-Party Relationships Involving Technology

This RFI highlights the challenge of defining what constitutes a "fintech." Historically, the term referred to nonbanks that offer financial services, often in competition with banks. Over time, however, the term has come to encompass a broader scope of companies that are viewed as bank partners rather than competitors. What constitutes a "fintech" partnership has taken many forms—ranging from traditional vendor relationships to white-labeling a third-party product to a tightly integrated go-to-market model. In each of these variations, the bank's goal is to improve efficiency and/or generate growth via new customer acquisition or new product sales.

The RFI's definition of fintech is both wide-ranging and unclear. It requests information regarding bank arrangements with "small- and medium-sized firms focused on the financial services sector as well as larger firms with established, multi-use technology platforms (sometimes referred to as "Big Tech")." The agencies explain that for purposes of the RFI, fintech companies "include, among many others intermediate platform providers…, as well as certain processors and payments platforms. It also includes certain non-financial retail businesses seeking to expand into markets for financial products and services through arrangements that could allow them to leverage their existing infrastructure and customer relationships to offer a one-stop-shop to access financial and non-financial products and services."

This definition indicates that the agencies intend the RFI to include banking as a service (BaaS) and embedded finance arrangements.[7] We also interpret the RFI to focus on retail customers, not institutional investors. But, it is less certain whether regulators view other types of third-party relationships, such as white-label arrangements, back-office technology service providers, or

---

[5] 89 Fed. Reg. 68244 (August 23, 2024).
[6] 89 Fed. Reg. 80135 (October 2, 2024).
[7] Banking-as-a-service is a model in which banks provide access to their core banking functions through application program interfaces (APIs). This enables fintechs to build their own financial products without needing to become banks. Embedded finance is the integration of financial services technology into platforms outside the financial sector. Through APIs, these platforms can offer services such as payments, loans, or insurance, making financial transactions part of the customer experience.

data aggregators[8] as constituting "fintech," and if so, whether there are appropriate differences in the treatment of those companies depending on the arrangement with the bank. Further muddying this concept, some vendors have rebranded and now market themselves as "fintech," when in fact there is nothing novel or cutting-edge about the product or service that they provide to the bank.

While the RFI's definition of "fintech" is unclear, we urge the agencies to identify factors in bank-fintech arrangements that involve increased risk, rather than defining "fintech." We do not believe that today's concept of fintech includes all technology-related vendors and payment processors.

In general, the more that a firm holds itself out to the public as providing bank-like services (as opposed to a core provider that serves only banks), the higher the risk that firm presents to end users and the banking system. Also, risks may stem from the specific role or function that the third party provides to the bank. Factors that may warrant closer risk management oversight include, for example, whether the fintech controls the customer relationship, conducts certain BSA/AML functions, controls account ledgers, or represents a significant concentration of the bank's deposits. Focusing on risks rather than specific types of providers will be more apt to future-proof any fintech-related guidance or rulemaking because the nature of fintechs themselves and the products and services they provide will change over time.

C. The Agencies Should Engage in Meaningful, Development-Stage Dialogue With All Stakeholders

Banks often find it useful to have proactive conversations with their examiners when exploring changes to their business strategies. Indeed, the agencies encourage this type of dialogue and transparency. These discussions provide examiners with a more fulsome understanding of the bank. And, banks can benefit from input regarding compliance, risk management, or other regulatory considerations that an examiner may identify.

This type of development-stage dialogue can be highly beneficial in the fintech context. However, some banks contemplating fintech partnerships have provided examiners with multiple briefings, yet received little to no input in return, leaving the banks guessing as to whether their plans would pass regulatory muster. In these situations, the lack of communication has been an impediment to innovation.

Development-stage communication helps to avoid situations where banks invest time and resources standing up a fintech partnership, only to subsequently abandon the initiative due to extensive regulatory scrutiny. This was the experience of one of our members whose examiners devoted dozens of hours to evaluating the bank's work on a fintech program, even though the bank had not even identified a prospective fintech partner. Ultimately, the bank abandoned the initiative due to its exam experience.

---

[8] We also note that it is unclear whether the agencies intend for data aggregators to fall within the scope of this RFI. The Joint Statement and the RFI are intertwined conceptually with the Consumer Financial Protection Bureau's implementation of Section 1033 of the Dodd-Frank Wall Street Reform and Consumer Protection Act, which provides that upon request by a consumer (or their agent), a consumer financial services provider must make information in the control or possession of the provider concerning the consumer financial product or service that the consumer obtained from the (subject to certain exceptions). Yet, neither the Joint Statement nor the RFI make any mention of this requirement.

The circumstances surrounding this bank's exam illustrate why some bankers and investors may believe that regulators automatically view bank-fintech partnerships as suspect and that banks will be subject to increased regulatory scrutiny simply for exploring innovative ways of working with fintech firms.[9] The agencies may be surprised by or disagree with this sentiment. But, we share it here to underscore the importance of regulatory transparency, including open dialogue and a well-communicated and risk-based approach to supervising bank-fintech arrangements.

Finally, it would be helpful if the agencies were to provide guidance regarding the point in time a bank should notify examiners that it is pursuing a fintech partnership. Banks do not want to be perceived as not informing examiners in a timely manner. At the same time, disclosing this information prematurely can lead to requests to produce draft documents and procedures that are incomplete or likely to change.

D. The Agencies Should Examine Partner Banks Based on the Structure of the Arrangement and the Risk Presented

Bank-fintech arrangements are not monolithic. They involve a wide range of structures and practices, some of which have evolved substantially in recent years. We discuss these developments in Section II., below.

We acknowledge and agree with regulators' historically risk-based approach to supervision. For this reason, are concerned that examiners appear to be applying a high and unwarranted degree of scrutiny to a broad universe of bank-fintech partnerships without regard to how the relationships are structured, the risks that they present, and the type and level of sophistication of the end-user (i.e., businesses vs. consumers). Factors that affect the risk associated with a partnership may include the bank's relationship and interactions with the end user, the allocation of responsibilities among parties (such as ledgering, compliance, and customer service), the presence of middleware, the risk mitigants and controls put in place by both the bank and its partner, the concentration of those activities relative to the broader business of the bank, and the contractual terms that govern the relationship. Likewise, all bank-fintech arrangements do not pose the same degree of complexity, or the same degree of potential liquidity, credit, or concentration risk. To be sure, some partnerships warrant closer supervision than others; however, several of our members have been subject to protracted examinations of their fintech partnerships, which may represent only a small portion of the overall activity at the bank and which did not culminate in significant findings or enforcement actions. This suggests that the exams were not properly scoped for risk in the first instance.

We urge the agencies to expressly acknowledge the range of bank-fintech structures and to commit to risk-based exams of these relationships. This risk-based approach should include an evaluation of whether potential risks are mitigated through current practices or regulation. Even though risk-based supervision is not a new concept and is fundamental to the Interagency Guidance on Third-Party Relationships,[10] we believe that an express statement that fintech-related exams will be risk-based is warranted, especially in light of the agencies' heightened focus on fintech partnerships in recent months.

---

[9] See also the February 2, 2024 letter from the House Financial Services Committee to FDIC Chairman Martin Gruenberg expressing concern that government agencies are "more interested in hindering innovation rather than helping it."
[10] 88 Fed. Reg. 37920 (June 9. 2023).

E. The Agencies Should Proactively Share Information With Banks on Examination Trends and Regulatory Concerns

The agencies issued the RFI and Joint Statement following a pronounced increase in enforcement actions involving banks with fintech partnerships. The Goodwin law firm found that between June 1, 2023, and June 30, 2024, the agencies issued more than 45 cease and desist orders that involved third-party risk management and/or fintech relationships or services.[11] Along these same lines, analysis by the Klaros group demonstrates the extent to which bank-fintech partnerships are driving supervisory priorities. Between the beginning of 2023 and early 2024, 25.6% of the FDIC's formal enforcement actions were issued to fintech partner banks. During the same period, 22% of the OCC's formal orders went to fintech partner banks. And,14% of the Federal Reserve's enforcement activity involved fintech partner banks.[12] In addition to public actions, we understand that partner banks are also facing an increased number of Matters Requiring Attention.

We urge the agencies to articulate clear expectations regarding fintech partnerships rather than continuing the ad hoc enforcement approach used to date. Prior to issuing the RFI and the Joint Statement, the agencies had not publicly explained their concerns regarding the specific types of risks that may be uniquely presented by bank-fintech partnerships. While various guidance documents, enforcement actions, and speeches by senior agency officials addressed these relationships in some capacity, the information provided was not specific to bank-fintech arrangements or was so high-level that its practical value was limited. The information provided in the Joint Statement and the RFI is an important initial step in providing more fulsome communications on this topic.

To further enhance transparency, we urge regulators to proactively share information with both banks and fintechs regarding identified risks, examination trends, and regulatory concerns. The agencies could communicate this information using both formal and informal mechanisms. For example, the CFPB's Supervisory Highlights, the FDIC's Supervisory Insights, or the Federal Reserve's Consumer Compliance Outlook serve as models of informal communication tools.[13] In addition to providing value to banks, this type of information could help fintechs to better understand key characteristics of successful bank-fintech partnerships.

We also request that the agencies issue formal guidance on fintech partnerships. This would be helpful on the front end of a partnership as banks consider how to structure the arrangement, assign roles and responsibilities, and negotiate contractual terms. In addition, as described in Section III. of this letter, banks typically leverage their existing enterprise risk management frameworks to identify and manage safety and soundness risks associated with fintech partnerships. To the extent that the agencies have identified weaknesses with this approach,

---

[11] Supervisory Experience and Enforcement Actions Continue to Drive Supervisory Priorities and Policy Development, August 8, 2024. https://www.goodwinlaw.com/en/insights/publications/2024/08/alerts-finance-ftec-supervisory-experience-and-enforcement-actions

[12] *See* https://www.klaros.com/post/who-s-been-toughest-on-fintech-partner-banks-recently-the-occ-federal-reserve-or-fdic; see also https://www.linkedin.com/posts/konrad-alt-12a7b35_sponsorbanks-enforcementactions-fintech-activity-7183876219917021185-qHID/

[13] The RFI includes a list of 27 existing regulatory guidance documents that apply to bank-fintech partnerships. This guidance applies to a variety of risk and compliance matters and is not focused on fintech partnerships. While this catalogue is helpful, information about trends and regulatory concerns associated to bank-fintech relationships would have a higher degree of practical value than a list of guidance documents.

they should share that information in a more transparent manner, including through regulatory guidance. Importantly, any formal guidance should be issued for advanced public notice and comment. Guidance that incorporates feedback from a wide range of stakeholders may be less susceptible to unpredictable policy shifts and changing regulatory expectations.[14]

Finally, we request that the Federal Reserve provide an update on the themes and trends that it has identified through its Novel Activities Supervision Program (NASP) and clarify the applicability and scoping of the program. For example, SR Letter 23-7 states that the program will apply to, among other things, projects that use distributed ledger technology "with the potential for significant impact on the financial system." In addition, banks "concentrated in providing traditional banking activities such as deposits, payments, and lending to crypto-asset-related entities and fintechs" will be covered by the NASP. We urge the Federal Reserve to explain what "significant impact on the financial system" and "concentrated in" mean for purposes of triggering the NASP. Likewise, we urge the Federal Reserve to provide examples of activities that are deemed to be outside of the scope of the NASP.

F. The Agencies Should Continue to Enhance Their Expertise

We encourage the agencies to take proactive steps to remain up-to-date as practices develop, including by meeting with banks and their fintech partners to discuss new partnership models. Expanding policymaker and examiner expertise pertaining to technology and innovation is central to the effective regulation of banks. This should be a priority in the digital age as banking practices and technology evolve.[15] A more forward-looking understanding of risks would also help to support innovation. Currently, risks are only identified on the back end of new innovations.

Engaging in informal discussions with banks and their fintech partners as well as experts from academia and other technology-related industries is one strategy for staying abreast of emerging developments. This could be accomplished in a myriad of ways, including by hosting regional townhalls (as has been done with capital and climate-related issues). The agencies could also assign staff to attend conferences attended by fintechs. In addition, each agency should establish and maintain an innovation office—if for no other reason than to ensure that regulations and supervisory practices are keeping up with technological and market developments.

The Federal Reserve's Novel Activities Supervision Program is one example of how cross-team collaboration might deepen an agency's understanding of technology and innovation matters. The goal of the program is to ensure that banks have a meaningful path to innovation, while helping regulators understand the risks of new initiatives. Under this program, a dedicated team of experts works with existing supervisory teams to examine novel activities conducted by supervised institutions (including complex, technology-driven partnerships with non-banks for the purpose of providing banking services). This collaboration has the potential to enhance the Federal Reserve's expertise regarding fintech partnerships and innovation more broadly. However, the Federal Reserve must balance this benefit with the reality that having more hands-on-deck risks creating inefficiencies that discourage banks from pursuing innovative products and services.

---

[14] In February 2024, the ABA issued a Whitepaper titled *Effective Agency Guidance* noting that, while notice-and-comment is not legally required for guidance, soliciting comment from the public helps promote the effectiveness of the guidance. This is because the failure to confer with regulated entities to understand interpretive questions, operational challenges, and system constraints often limits the utility of guidance.

[15] This point is underscored by a 2023 report by the General Accountability Office and a 2024 letter from the House Financial Services Committee to the FDIC.

We understand that FDIC and the OCC also have examiners with expertise in fintech and innovation. For example, the FDIC oversees industrial banks, and as a result, has a group of examiners with an emphasis in fintech and bank partnerships. The OCC also has specialized technology examiners as well as a division of quantitative experts that focus on the algorithms used by large banks and fintechs. We urge the FDIC and the OCC to describe how they leverage the expertise of both experts and supervisory staff to enhance supervision of innovation-related matters. This would increase public confidence regarding the FDIC's and OCC's commitment to modern supervision and the professional development of agency staff.

Innovation is changing both banking and the broader economy, and the pace of change will only continue to increase. As a result, an innovation focus should become business as usual for all agencies, with training that is regularly updated to help examination staff remain current. We also suggest that the agencies establish a feedback loop between field examiners and agency leadership on innovation topics.

G. The Agencies Should Conduct External Education and Outreach

In addition to building their own knowledge, the agencies can play an important role in educating fintechs and bank directors about bank regulation and supervision and the associated expectations that apply to bank-fintech partnerships. A discussion of potential risks and expected board oversight would also be valuable.

The OCC's Office of Innovation (later expanded by the Office of Financial Technology) has provided meaningful outreach and technical assistance to fintechs, including by hosting virtual office hours. But, like any successful communications strategy, this work would benefit from being delivered via more channels and over a longer period of time. This may improve fintech awareness of what is required to form successful partnerships with banks. Many early-stage fintechs still do not understand regulatory and risk management expectations, and, by extension, how those requirements must be addressed within bank-fintech partnerships. In addition, many fintechs do not understand that a bank's appetite for partnership will be influenced by the extent to which a fintech is willing to help a bank meet regulatory expectations.

Finally, expanding the OCC's workshops for community bank directors and senior management could serve as an additional vehicle for providing outreach and education. These programs provide valuable content to directors and senior management seeking to review banking fundamentals or receive updates on emerging issues. The topic of bank-fintech partnerships would be a beneficial addition to the workshop series, especially as recent enforcement actions have underscored the importance of board oversight of fintech arrangements.

H. The Agencies Should Address Risks Based on Where They Lie

To date, regulators have expected banks to oversee third parties as if the activity or service the third party provides is being performed by the bank itself. This expectation extends to bank-fintech partnerships. As a practical matter, it places banks in the position of being de facto regulators of fintechs.

While banks must comply with applicable laws and regulations and must conduct due diligence on and otherwise manage their third parties, banks are not supervisors and should not be the primary entities responsible for overseeing fintech practices. Relying on banks to police fintech conduct is not an effective or efficient way to ensure that fintechs comply with applicable laws and regulations. This is especially true with respect to ascertaining whether fintech models raise fair banking issues, as banks often cannot get visibility into fintech models because the models constitute proprietary information. Furthermore, fintechs often have relationships with multiple banks. Requiring fintechs to submit to duplicative monitoring and oversight by each bank partner is burdensome for the fintech.

A more efficient and effective means to address fintechs' compliance is through the Bank Service Company Act (BSCA). The BSCA provides the FDIC, Federal Reserve, and OCC with statutory authority to examine and regulate the performance of certain services provided by third-party providers. The agencies' examination authority does not extend to services not covered under the BSCA or to a service provider's business more generally. We urge the agencies to exercise this authority with respect to a broader universe of fintechs. While the agencies have used their BSCA authority to issue enforcement actions against financial technology firms, they have backed away from this approach in recent years.[16]

As a practical matter, regulators do not examine all service providers covered by the BSCA. Whether a service provider is examined (as well as the frequency and priority of any such examination) is based on a case-by-case analysis of the criticality of the service, the number of financial institutions under contract with the service provider, and the inherent risk that the service may present to client financial institutions, among other considerations.

Moreover, although BSCA examinations result in an examination report, banks have varying degrees of success in obtaining these reports in a timely manner. Banks may factor these examination reports into their approach for managing a particular third party. However, many banks find the value of these reports to be limited due to the substantial lag time between the date of the exam and the date by which the regulator provides the exam report to the bank.[17]

Although the BSCA has limits, calls have recently come from both sides of the political aisle for the agencies to do more in this regard. In September 2024, Senators Warren and Van Hollen called on the agencies to regulate fintechs directly.[18] Similarly, in a July 2024 speech, Acting Comptroller Hsu acknowledged the agencies' BSCA authority, but observed that the continued evolution of bank-non-bank arrangements "has highlighted the need for more granular approaches and greater engagement between the [federal banking agencies] and nonbank fintechs." And, in February 2024, Federal Reserve Governor Michelle Bowman identified regulatory oversight of third-party service providers pursuant to the BSCA as a potentially underused tool that the agencies could use to align "supervisory attention with the source of risk."[19]

ABA believes that a modern economy and modern banking system demand an efficient and effective approach to supervision. Relying on individual banks to ensure that fintechs comply

---

[16] See the See the Federal Reserve Cease and Desist Order against Higher One Incorporated https://www.federalreserve.gov/newsevents/pressreleases/enforcement20151223a.htm, Interagency Consent Order against MERS Corp. https://www.occ.gov/news-issuances/news-releases/2011/nr-occ-2011-47h.pdf, and the FDIC settlement with CompuCredit https://archive.fdic.gov/view/fdic/3338.

[17] Currently, banks must request regulators to provide a copy of the service provider's exam report. Banks are frustrated by the difficulty of knowing which service providers have been examined, and by extension, knowing which examination reports to request.

[18] https://www.warren.senate.gov/imo/media/doc/warren_van_hollen_letter_to_prudential_regulators_on_baas_oversight_91124.pdf

[19] https://www.federalreserve.gov/newsevents/speech/bowman20240202a.htm

with applicable laws and regulations does not achieve this objective. And, as a practical matter, community banks are unlikely to possess sufficient market power to influence fintech behavior. For this reason, we urge the banking agencies to leverage their existing authority under the BSCA to oversee fintech firms and to identify areas where the scope of covered BSCA activities may need to be expanded. Given the BSCA's limits, the agencies may need additional statutory authority to oversee the full panoply of bank-fintech partnerships.

We note that the Consumer Financial Protection Bureau (CFPB) is taking a more active role in supervising non-depository covered persons pursuant to section 1024 of the Consumer Financial Protection Act.[20] In April 2022, the CFPB announced it would use its authority to start supervising nonbanks that pose risks to consumers, and mentioned fintechs as an example in its announcement.[21] In addition, in November of 2023, the CFPB issued a proposed rule that would establish supervisory authority over large nonbank providers of general use digital payment applications. We support this increase in the supervision of nonbanks.

II. Range of Practices and Evolution of Fintech Partnerships

Bank-fintech arrangements are not homogenous and can vary from bank to bank and fintech to fintech. They involve a wide range of models—some of which have evolved substantially over time. None of these models is inherently good or bad. Rather, the structure of each model and its assignment of roles, responsibilities, and controls among the participants presents different risks that should be managed and examined accordingly. Notably, some bank-fintech arrangements have changed in recent years to include new structures and new approaches to allocating responsibilities among the parties. These developments illustrate why the RFI and continued dialogue about innovation and new models for bank-fintech partnerships is important.

Below, we discuss some of the most common types of bank-fintech arrangements, which could include partnerships or other types of arrangements. We do not discuss the full universe of these relationships, and we anticipate that additional use cases will emerge over time as both technology and the economy evolve.

<u>Payments</u>. Bank-fintech arrangements for the purpose of facilitating payments are among the oldest types of bank-fintech relationships. In one common model, a bank sponsors another entity (either a bank or a non-bank) for the purpose of offering a card program. Co-branded credit card programs are a variation of this arrangement where a non-bank partners with a bank to issue a credit card under the non-bank's brand. Co-branded credit cards are particularly common in the travel and retail industries. Another example of a payment arrangement is a non-bank peer-to-peer platform offered by a licensed money transmitter that has a customer relationship with a bank in order to complete financial transactions. In each of these cases, the non-bank delivers a financial service under its own brand using the bank's infrastructure.

Payroll processing is also a longstanding business model that involves non-bank third parties initiating payments. In this scenario, a business hires a vendor to manage payments to employees through the Automated Clearing House (ACH). The vendor delivers payment files to the business's bank in order to originate payments to the business's employees. The bank submits those payments to the ACH network and the funds are transmitted to the employees'

[20] 12 U.S.C. 5514.
[21] https://www.consumerfinance.gov/about-us/newsroom/cfpb-invokes-dormant-authority-to-examine-nonbank-companies-posing-risks-to-consumers/

bank. The business, the non-bank vendor, and the business's bank have an agreement on how the process works and the bank warrants that the payments are authorized.

This situation can also involve ACH debits where the business employs a vendor to manage incoming payments. Common examples include health club membership dues or subscriptions. In this scenario, the non-bank third party provides a payment file with the ACH debits to the business's bank for processing. The bank warrants that the debits are authorized to be paid to the business by the customer. These scenarios are conducted under contractual agreement and have been in place long before the term "fintech" came into use.

Another example of third-party payment providers are payment facilitators ("payfacs"), which enable fintechs to provide their clients with the ability to accept card payments. Payfacs may open a custodial, "for benefit of" account with a bank in order to settle transactions. As with other types of third-party payment relationships described above, this type of bank-third party relationship is not novel.

<u>Deposit Generation</u>. Bank-fintech partnerships for the purpose of deposit-taking is a newer model. The details of these partnerships vary significantly based on the extent to which the bank has a direct relationship with the end user.

Indirect Model. On one end of the spectrum, a fintech operates a seemingly standalone financial services company and has the primary relationship with end users. In addition to serving as a channel partner for the bank, the fintech may support some servicing of the customer, including providing the technology interface through which the customer initiates transactions or reviews his or her accounts. The fintech or a middleware provider may also assume certain compliance functions and serve as the primary point of contact for customer service inquiries. This is sometimes referred to as an "indirect" model.

The type of deposit account in which end user funds are held is a defining feature of this model. Instead of each end user having an individual deposit account at the bank, the fintech often holds end user deposits in an omnibus custodial account. Rather than creating separate deposit accounts for each individual customer, the fintech may pool funds belonging to thousands of customers into a single account at the partner bank. The fintech company serves as the custodian of the funds placed at the bank on behalf of its many customers, who are the actual owners of the funds. The fintech tracks each end user's funds on a synthetic ledger. End users in this scenario may believe that they are "banking" with the fintech.[22]

If properly documented and accounted for, end-user funds in custodial accounts may qualify for FDIC deposit insurance in the event that the partner bank fails. These arrangements may provide for "pass-through" insurance—where the insurance passes through the custodian to protect each end user.

Direct Model. In contrast to the indirect model, some banks have adopted a "direct" model where the bank—not the fintech—holds the principal relationship with the end user. This type of arrangement is sometimes referred to as a virtual or digital branch. In these arrangements, each

[22] It should be noted, however, that not all bank-fintech arrangements that include an omnibus account titled in the name of the fintech for the benefit of the fintech's customers should be considered a deposit-generation partnership. Various models and use cases exist for banks to open omnibus accounts holding third party funds for various purposes, as noted in the regulatory initiatives listed in Section I.

end user has an individual deposit account at the bank. (The fintech does not pool end user funds in an omnibus custodial account as with the indirect model). The fintech's application serves as the end user's point of entry into the bank and is similar to a marketing engine that supports the bank's customer acquisition. Other than serving as the channel through which the customer is acquired, the end user's relationship with the bank is the same as any other bank customer. In some cases, the fintech provides service to the bank; it does not interact with the end user in the place of the bank. In other cases, the fintech continues to handle customer interactions while the bank still maintains an individual account with the customer.

The process for onboarding customers that enter a banking relationship via the fintech app is identical to the process that applies to customers that open an account at a bank branch. The only difference is that the account opening process occurs via the fintech's mobile app. The fintech provides tech services only and does not have the ability to open or close the account. This is not a passive relationship where the bank builds deposits and takes fee income.

In addition to having a different deposit account structure and a more direct relationship with end users, some banks have chosen to move customer service and compliance-related functions in house rather than outsourcing them to the fintech or a middleware provider. This includes, for example, conducting fraud monitoring, establishing ACH and wire transfer limits, providing consumer disclosures, and performing certain functions related to anti-money laundering and countering the financing of terrorism (AML/CFT). Banks cite multiple reasons for this shift, including the ability to provide an enhanced customer service experience and reduce the risk that the bank will be charged with a regulatory violation due to noncompliance by the fintech.[23] In particular, these banks are mindful of the need to continuously evaluate their AML/CFT risks and corresponding controls associated with the fintech arrangement.

This direct model may provide notable benefits for banks that have the financial resources and access to talent required to implement it. But, not all banks have the investment dollars or staff expertise to build the systems required to connect to fintechs directly or to handle the compliance and operational responsibilities associated with a marked increase in accounts generated via a fintech channel. For this reason, regulators should not discourage banks from pursuing an indirect partnership model, as long as the arrangement is appropriately monitored and controlled. Banks of all sizes and financial capabilities must be able to innovate and provide financial products and services in new ways.

III. Risks Presented and Techniques for Managing Them

Both the RFI and the Joint Statement describe risks that can be associated with fintech partnerships. Below, we provide additional information and commentary on a select number of these risks.

A. Expertise

Bank-fintech partnerships are not passive "plug and play" arrangements. Both banks and their fintech partners should have sufficient expertise to carry out their respective partnership responsibilities, based on the size, scope, and complexity of those underlying activities. Bank staff should have the skills to thoroughly assess the risks presented by the relationship, design

[23] Even though a fintech may have a contractual responsibility to perform certain AML/CFT functions, a bank cannot contract away its AML/CFT compliance obligations, as the bank remains accountable for adhering to AML/CFT regulations and sanctions requirements, even when working with a fintech partner.

effective controls, and perform adequate oversight. Similarly, depending on the arrangement, fintech staff that does not have banking expertise may be a red flag for potential bank partners, particularly if the fintech will perform compliance-related functions on behalf of the bank.

B. Consumer Protection

Bank-fintech arrangements can present consumer protection risks, including the risk of inaccurate or improper disclosures, discrimination, unfair or deceptive acts or practices, and privacy concerns.

Consumer Disclosures. Banks are responsible for ensuring that their customers receive the requisite account disclosures, regardless of whether the partnership's contractual terms task the bank or the fintech with providing this information to the end user. Some fintechs lack a fulsome understanding of the consumer disclosure requirements with which banks must comply. For this reason, many banks with an indirect partnership model require that all consumer protection-related disclosures be based on bank policies and be approved by all of the bank's internal stakeholders (e.g., compliance, fair lending, legal, etc.). The bank either drafts the disclosures or, if the fintech drafts them, the bank must approve the language pursuant to an established process. The fintech is prohibited from changing a disclosure without obtaining bank signoff. In situations where a customer relationship is generated by the fintech but the bank manages all compliance functions internally, banks commonly use the same disclosures that they use for customers who enter the bank through traditional channels.

Fintechs that provide payments services through a bank can create additional risks to consumers because consumers may not fully understand that they have different risks and rights when a fintech moves funds from the consumer's bank account to the fintech's account. Fintechs that provide money movement services and/or act as digital wallet operators should adopt a more robust risk management framework and fraud prevention controls.

Fair Lending. Fintechs may pose novel risks for fair lending. For example, they may use alternative data sources and automated models for marketing, underwriting, and pricing that provide end users with faster and more cost-effective access to credit. These tools may make it possible to extend responsible and fair access to credit to more consumers who do not have a traditional credit history. These tools are in the early stages of development and there are concerns that they may be susceptible to bias and inaccuracy. This concern is compounded by the fact that fintechs often do not provide sufficient transparency into their models and data sources so that banks can conduct fair lending analysis and testing during the due diligence phase of the relationship.

For example, banks of all sizes encounter due diligence and oversight challenges associated with fintech underwriting models. Fintechs rarely assist with model validation and share information only begrudgingly, if at all. In addition, the models are increasingly complex, which compounds these challenges. Banks attempt to include contractual language requiring fintechs to be transparent, but fintechs often do not agree to these provisions, citing the need to protect their proprietary information. Further, community banks often lack the market power to negotiate model transparency language.

Banks that elect to pursue a relationship with a fintech that utilizes these types of models may conduct recurring transaction testing on a sample of loan transactions to ensure that the fintech model does not produce discriminatory results. This approach is inefficient, as each bank that utilizes the fintech model must conduct the same routine testing. Some banks engage outside counsel, consultants, or an audit firm to review fintech credit models and marketing practices both as part of the due diligence phase and then periodically thereafter. These engagements are costly and impact the value proposition of certain types of bank-fintech partnerships. As discussed in Section I., above, we urge the agencies and/or the CFPB to take a more active role in overseeing fintechs that utilize these types of models.

C. Data Access and Privacy

Bank-fintech partnerships often raise questions about data ownership and use. As with other risks presented by fintech partnerships, banks handle privacy and data sharing issues in a variety of ways. Usually, they negotiate and manage privacy and data access issues based on the structure of the partnership and the service(s) that the fintech provides. At the same time, technology is evolving rapidly in terms of how information is shared, and banks are increasingly consulting with both inside and outside counsel on privacy and data sharing matters pertaining to their fintech partnerships.

A common scenario involving questions of data ownership and use arises where a fintech collects extensive information from an end user before the end user becomes a customer of the bank. This may include information about the end user's browsing on the fintech's website or information that is part of the end user's incomplete application. (Complete applications are subject to bank privacy requirements and policies). The fintech company may view this type of information as proprietary and attempt to limit the bank's access to it.

Another issue related to data ownership and use arises where banks are required by law to limit the fintech's access to and use of certain data. For example, banks are restricted in the sharing and use of end user nonpublic information, and end users may have opt-out rights, which could pose operational difficulties and compliance risks. In this situation, banks usually require that the fintech comply with the bank's policies and procedures. This scenario typically arises where the fintech has contractually agreed to assume compliance responsibilities associated with the account and the end user is not a named account holder with the bank.

Finally, it is possible for the bank and the fintech to separately own the same information. This can occur where the fintech offers products and services that are independent of its relationship with the partner bank. These situations can be difficult to negotiate. Some banks have secured contractual provisions that require the fintech to separately designate in the fintech's platform what information belongs to the bank and what information belongs to the fintech. But, this can be difficult—especially in the lead up to an end user becoming a bank customer. And, it can be further complicated, for example, if the fintech is servicing the bank's loan as well as providing its own services on the same platform. If the data is comingled, banks audit the fintech's use of the data to ensure that it is not being used for marketing or other impermissible purposes.

D. Ledgering and Access to Records

Some risk is created when a fintech or middleware provider is responsible for account ledgering on a bank's behalf, and the bank must manage that risk accordingly.[24] This is the indirect model described in Section II. of this letter. Contracts governing these arrangements should specify which party is responsible for account ledgering. If these records are maintained by the fintech or a middleware provider, the bank should have sufficient access to the deposit and transaction

[24] State law may require a fintech to maintain the ledger in arrangements involving money transmission.

system of record and know who the end users are. It is also prudent to be able to identify and track which custodial accounts are tied to each fintech partner and program.

Direct arrangements—where each end user has an individual account at the bank—may not present concerns about ledgering and data access, particularly if the bank uses the same deposit and transaction system of record that it utilizes for customers who initiate a banking relationship through traditional channels. Regulators should take these differences into account when scoping exams involving bank-fintech partnerships.

On October 2, 2024, the FDIC issued a proposed rule purportedly in response to the Synapse bankruptcy that would impose new recordkeeping requirements on custodial accounts held by insured depository institutions. The proposed rule addresses the indirect model of deposit-generating fintech partnerships. Because we are still analyzing the FDIC's proposal, we do not comment further here regarding ledgering issues. However, we will submit comments on the proposed rule on or before the comment deadline.

E. Safety and Soundness Risk

The RFI poses multiple questions about how banks address safety and soundness risk associated with fintech partnerships. Banks typically leverage their existing enterprise risk management (ERM) frameworks to identify and manage these risks, such as rapid growth, liquidity, and concentration risk. This includes establishing risk limits and tracking mechanisms. And, in the case of deposit-generating partnerships, banks are mindful of concentrations and structure fintech accounts to avoid large deposit outflows on any given day, month or longer period of time, in accordance with standard liquidity risk management practices. ERM frameworks also include governance structures that help to confirm that growth is adequately supported. Finally, banks use their board-approved strategic plans to specify their appetite for and desired pace of growth via fintech partnerships.

To the extent that the agencies have identified weaknesses with this approach, they should share that information in a more transparent manner, including through regulatory guidance.

F. Wind-Down Scenarios

A well-thought-out plan dealing with the termination of a bank-fintech partnership is another important tool for managing concentration and liquidity risk. A wind-down situation may occur where the fintech becomes insolvent or decides to transfer its business to another bank partner. It may also occur when the bank elects to end the partnership. As with many issues presented by fintech partnerships, the impacts of these scenarios will depend on the structure, size, and complexity of the partnership, as well as whether the bank has a direct relationship with the end user.

For example, potential liquidity risk presented in the wind down of a direct model deposit-generating partnership (i.e., the end user has an individual deposit account at the bank) may differ from the liquidity risk presented by the indirect model involving omnibus custodial accounts that the fintech can unilaterally move to another bank.

The termination of a fintech partnership operating under the direct model is akin to a bank branch burning down. The end user's point of entry into the bank may be gone, but the bank still owns the customer relationship. The fintech does not control the deposit agreement and cannot close the depositor's account. The fintech may attempt to incentivize the depositor to follow the fintech to a new partner bank, but this can be a time consuming and costly process for the fintech, as it would require untangling the end user's banking arrangements. This could be cumbersome, particularly if a commercial end user has integrated its deposit account with Quickbooks. While the CFPB's recent rulemaking on consumer access to financial records may mitigate some of these hurdles, various account opening agreements and authorizations will still be required before a consumer is able to use the account with a new partner bank.

Banks employing the indirect model have negotiated contractual language at the outset of the partnership that specifies which party will own the customer upon termination or insolvency of the fintech. Some banks have negotiated contractual language specifying that end-user accounts would transfer to the bank. Other common wind down provisions include an exit or breakup fee, a fee payment to match the trailing 12-24 months of the program, and/or non-solicitation provisions.

G. Contractual Considerations

Over the years, banks have encountered a myriad of challenges when negotiating contracts with fintechs. This is sometimes due to fintechs lacking awareness of or experience with the regulatory requirements, prudential expectations, and supervisory scrutiny to which banks are subject. The situation has improved somewhat, due to the educational outreach conducted by both banks and the OCC and publicity generated by the uptick in enforcement actions against partner banks. However, multiple pain points remain.

For example, start-up firms sometimes resist responding to expensive due diligence requests or obtaining a System and Organization Controls (SOC) report. Some of our members have walked away from pursuing deals with fintechs in these situations. In addition, some fintechs refuse to agree to indemnification provisions, particularly those that address data breaches and intellectual property infringement.

Banks' ability to access and review fintech models also remains a significant challenge. Historically, fintechs have denied banks access to their models, claiming that the models constitute proprietary information. If a bank elects to pursue the relationship, it must regularly back-test a sample of transactions to ensure that the fintech model does not produce discriminatory results. This approach is inefficient, as each bank that utilizes the fintech model must conduct the same testing on an ongoing basis. Regulators can support innovation and the evolution to a modern banking system by leveraging their BSCA authority (or working with Congress to obtain expanded authority) to examine models developed by fintech firms.

Banks also find it difficult to negotiate with data aggregators, particularly with respect to data security issues and liability in the event of a data breach. It is also challenging for banks to obtain information about fourth parties and downstream data uses. The role of data aggregators may continue to evolve now that the CFPB has finalized its rulemaking on consumer access to financial records. As discussed earlier in this letter, it is unclear whether the agencies intended to cover data aggregators within the scope of this RFI.

A bank and a data aggregator may enter into a contract that establishes the criteria that the data aggregator must meet in order to access customer data. Such a contract does not result in the data aggregator becoming a third-party service provider to the bank. In these situations, banks share information with the aggregator at the direction of the bank's customer. Yet, aggregators are of the view that they should not be liable in the event of a data breach.

Conclusion

We appreciate the opportunity to comment on this RFI. Banks must have a meaningful path to innovation, and the RFI is an important step in developing a transparent and cohesive approach to regulating and supervising bank-fintech partnerships. We look forward to continued engagement on these critical issues.

Sincerely,

Krista Shonk
SVP & Sr. Counsel
Fair and Responsible Banking
Regulatory Compliance and Policy