DEPARTMENT OF THE TREASURY

Office of the Comptroller of the Currency

[Docket No. OCC–2024–0014]

FEDERAL RESERVE SYSTEM

[Docket No. OP–1836]

FEDERAL DEPOSIT INSURANCE CORPORATION

RIN 3064–ZA43

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

AGENCY: Office of the Comptroller of the Currency, Treasury; Board of Governors of the Federal Reserve System; and Federal Deposit Insurance Corporation.

ACTION: Request for information and comment.

SUMMARY: Over the past several years, the Office of the Comptroller of the Currency (OCC), Treasury; the Board of Governors of the Federal Reserve System (Board); and the Federal Deposit Insurance Corporation (FDIC) (collectively, ''the agencies'' or ''agency'' when referencing the singular) have observed and reviewed arrangements between banks and financial technology (fintech) companies. The agencies support responsible innovation and banks pursuing bank-fintech arrangements in a manner consistent with safe and sound banking practices, and with applicable laws and regulations, including consumer protection requirements and those addressing financial crimes. Bank-fintech arrangements can provide benefits; however, supervisory experience has highlighted a range of potential risks with these bank-fintech arrangements. This request solicits input on the nature of bank-fintech arrangements, effective risk management practices regarding bank-fintech arrangements, and the implications of such arrangements, including whether enhancements to existing supervisory guidance may be helpful in addressing risks associated with these arrangements.

DATES: Comments must be received on or before September 30, 2024.

ADDRESSES: Comments should be directed to:

OCC: Commenters are encouraged to submit comments through the Federal eRulemaking Portal, if possible. Please use the title ''Request for Information on Bank-Fintech Arrangements Involving Banking Products and Services Distributed to Consumers and Businesses'' to facilitate the organization and distribution of the comments. You may submit comments by any of the following methods:

- *Federal eRulemaking Portal—Regulations.gov:* Go to *https://www.regulations.gov.* Enter ''Docket ID OCC–2024–0014'' in the Search Box and click ''Search.'' Public comments can be submitted via the ''Comment'' box below the displayed document information or by clicking on the document title and then clicking the ''Comment'' box on the top-left side of the screen. For help with submitting effective comments, please click on ''Commenter's Checklist.'' For assistance with the *Regulations.gov* site, please call 1–866–498–2945 (toll free) Monday–Friday, 8:00 a.m. to 7:00 p.m. ET, or email *regulationshelpdesk@gsa.gov.*
- *Mail:* Chief Counsel's Office, Attention: Comment Processing, Office of the Comptroller of the Currency, 400 7th Street SW, Suite 3E–218, Washington, DC 20219.
- *Hand Delivery/Courier:* 400 7th Street SW, Suite 3E–218, Washington, DC 20219.

Instructions: You must include ''OCC'' as the agency name and ''Docket ID OCC–2024–0014'' in your comment. In general, the OCC will enter all comments received into the docket and publish the comments on the *Regulations.gov* website without change, including any business or personal information provided such as name and address information, email addresses, or phone numbers. Comments received, including attachments and other supporting materials, are part of the public record and subject to public disclosure. Do not include any information in your comment or supporting materials that you consider confidential or inappropriate for public disclosure.

You may review comments and other related materials that pertain to this action by the following method:

- *Viewing Comments Electronically—Regulations.gov:* Go to *https://regulations.gov/.* Enter ''Docket ID OCC–2024–0014'' in the Search Box and click ''Search.'' Click on the ''Dockets'' tab and then the document's title. After clicking the document's title, click the ''Browse All Comments'' tab. Comments can be viewed and filtered by clicking on the ''Sort By'' drop-down on the right side of the screen or the ''Refine Comments Results'' options on the left side of the screen. Supporting materials can be viewed by clicking on the ''Browse Documents'' tab. Click on the ''Sort By'' drop-down on the right side of the screen or the ''Refine Results'' options on the left side of the screen checking the ''Supporting & Related Materials'' checkbox. For assistance with the *Regulations.gov* site, please call 1–866–498–2945 (toll free) Monday–Friday, 8:00 a.m. to 7:00 p.m. ET, or email *regulationshelpdesk@gsa.gov.*

The docket may be viewed after the close of the comment period in the same manner as during the comment period.

Board: You may submit comments, identified by Docket No. OP–1836, by any of the following methods:

- *Agency Website: https://www.federalreserve.gov/.* Follow the instructions for submitting comments at *https://www.federalreserve.gov/apps/foia/proposedregs.aspx.*
- *Email: regs.comments@federalreserve.gov.* Include the OMB number or FR number in the subject line of the message.
- *Fax:* (202) 452–3819 or (202) 452–3102.
- *Mail:* Federal Reserve Board of Governors, Attn: Ann E. Misback, Secretary of the Board, Mailstop M–4775, 2001 C St. NW, Washington, DC 20551.

All public comments are available from the Board's website at *https://www.federalreserve.gov/apps/foia/proposedregs.aspx* as submitted, unless modified for technical reasons or to remove personally identifiable information at the commenter's request. Accordingly, comments will not be edited to remove any confidential business information, identifying information, or contact information. Public comments may also be viewed electronically or in paper in Room M–4365A, 2001 C St. NW, Washington, DC 20551, between 9:00 a.m. and 5:00 p.m. on weekdays, except for Federal holidays. For security reasons, the Board requires that visitors make an appointment to inspect comments. You may do so by calling (202) 452–3684. Upon arrival, visitors will be required to present valid government-issued photo identification and to submit to security screening in order to inspect and photocopy comments.

FDIC: You may submit comments, identified by RIN 3064–ZA43, by any of the following methods:

- *Agency Website: https://www.fdic.gov/resources/regulations/federal-register-publications/.* Follow instructions for submitting comments on the FDIC's website.
- *Email: Comments@fdic.gov.* Include ''Request for Information on Bank-Fintech Arrangements Involving Banking Products and Services Distributed to Consumers and

Businesses/RIN 3064–ZA43'' in the subject line of the message.

• *Mail:* James P. Sheesley, Assistant Executive Secretary, Attention: Request for Information on Bank-Fintech Arrangements Involving Banking Products and Services Distributed to Consumers and Businesses—RIN 3064–ZA43, Federal Deposit Insurance Corporation, 550 17th Street NW, Washington, DC 20429.

• *Hand Delivery:* Comments may be hand-delivered to the guard station at the rear of the 550 17th Street NW, building (located on F Street NW) on business days between 7:00 a.m. and 5:00 p.m. ET.

• *Public Inspection:* Comments received, including any personal information provided, may be posted without change to *https://www.fdic.gov/resources/regulations/federal-register-publications/.* Commenters should submit only information that the commenter wishes to make available publicly. The FDIC may review, redact, or refrain from posting all or any portion of any comment that it may deem to be inappropriate for publication, such as irrelevant or obscene material. The FDIC may post only a single representative example of identical or substantially identical comments, and in such cases will generally identify the number of identical or substantially identical comments represented by the posted example. All comments that have been redacted, as well as those that have not been posted, that contain comments on the merits of this notice will be retained in the public comment file and will be considered as required under all applicable laws. All comments may be accessible under the Freedom of Information Act.

FOR FURTHER INFORMATION CONTACT:

OCC: Miriam Bazan, Financial Technology Policy Specialist, or Tracy Chin, Director for Payment Systems Policy, Bank Supervision Policy (202) 649–5200; or Beth Knickerbocker, Special Counsel, Micah Cogen, Counsel, or Graham Bannon, Counsel, Chief Counsel's Office (202) 649–5490. If you are deaf, hard of hearing, or have a speech disability, please dial 7–1–1 to access telecommunications relay services.

Board: Kavita Jain, Associate Director, Novel Activities and Innovation Policy, (202) 452–2062, Jeff Ernst, Manager, Innovation Policy, (202) 452–2814, or Roman Goldstein, Lead Financial Institution Policy Analyst, (202) 452–3802, Division of Supervision and Regulation; Drew Kohan, Associate Director, Program Direction, Division of Consumer and Community Affairs, (202) 452–3040; Asad Kudiya, Deputy Associate General Counsel, (202) 475–6358 or Isabel Echarte, Attorney, (202) 452–2514, Legal Division, Board of Governors of the Federal Reserve System, 20th and C Streets NW, Washington, DC 20551. For the hearing impaired only, Telecommunication Device for the Deaf (TDD), (202) 263–4869.

FDIC: Rae-Ann Miller, Senior Deputy Director, (202) 898–3898, or Tom Lyons, Associate Director, (202) 898–6850, Division of Risk Management Supervision; Luke Brown, Associate Director, (202) 898–3842, or Meron Wondwosen, Chief, (571) 438–7127, Division of Depositor and Consumer Protection; Annmarie Boyd, Senior Counsel, (202) 898–3714, or Vivek Khare, Senior Counsel, (202) 898–6847; FDIC, 550 17th Street NW, Washington, DC 20429; FDIC, 550 17th Street NW, Washington, DC 20429.

SUPPLEMENTARY INFORMATION:

Background Information

The agencies are responsible for supervising certain Federally-chartered and State-chartered banks (herein referred to as ''banks'').[1] Over the past several years, the agencies have observed and reviewed arrangements between banks and fintech companies [2] that provide consumers and businesses (herein referred to as ''end users''), access to banking products and services. Although these arrangements may provide benefits, supervisory experience has highlighted a range of risks with these bank-fintech arrangements. The agencies support responsible innovation and support banks in pursuing bank-fintech arrangements in a manner consistent with safe and sound practices and applicable laws and regulations, including but not limited to, consumer protection requirements (such as fair lending laws and prohibitions against unfair, deceptive, or abusive acts or practices) and those addressing financial crimes (such as fraud and money laundering).[3] This request solicits input on the nature of bank-fintech arrangements, including their benefits and risks, effective risk management practices regarding bank-fintech arrangements, and the implications of such arrangements, including whether enhancements to existing supervisory guidance may be helpful in addressing risks associated with these arrangements.

For many years, non-banks have provided access to financial products and services, such as consumer credit products, commercial loans, payment products, and deposit accounts. Rapid technological advances and evolving customer preferences are accelerating these trends. Over the past decade, fintech companies have significantly expanded their ability to distribute financial products and services directly to end users. These companies include small- and medium-sized firms specifically focused on the financial services sector as well as larger firms with established, multi-use technology platforms (sometimes referred to as ''Big Tech''). For purposes of this Request for Information (RFI), we refer to all of these types of non-bank firms as ''fintech companies.'' [4]

To facilitate providing end users with access to banking products and services, fintech companies may enter into arrangements with banks. In these arrangements, a bank typically makes products or services available through an arrangement with one or more fintech companies in which the fintech company, rather than the bank, markets, distributes, or otherwise provides access

[1] For a description of the banks supervised by each agency and relevant to this request for information, refer to the definition of ''appropriate Federal banking agency'' in the Federal Deposit Insurance Act (12 U.S.C. 1813(q)(1), (2), and (3)(A)–(E)).

[2] In some cases, the fintech company may be an affiliate of the bank, such as, for example, where a bank holding company owns a fintech, and that fintech relies on the holding company's subsidiary bank to provide end users access to banking products or services.

[3] Examples of relevant issuances may include the following: Interagency Guidance on Third-Party Relationships: Risk Management, 88 FR 37920 (Jun. 9, 2023); Interagency Guidelines Establishing Information Security Standards, 70 FR 15736 (Mar. 29, 2005); Interagency Guidelines Establishing Standards for Safety and Soundness, 61 FR 43948 (Oct. 1, 1996); FDIC FIL–15–2024, Collecting Identifying Information Required Under the Customer Identification Program (CIP) Rule (Mar. 28, 2024); Third-Party Risk Management: A Guide for Community Banks (May 2024); Conducting Due Diligence on Financial Technology Companies: A Guide for Community Banks (Oct. 2023); FDIC FIL–35–2022, Advisory to FDIC-Insured Institutions Regarding Deposit Insurance and Dealings with Crypto Companies (July 20, 2022); Joint Statement on the Risk-Based Approach to Assessing Customer Relationships and Conducting Customer Due Diligence (July 6, 2022); Interagency Guidance to Issuing Banks on Applying Customer Identification Program Requirements to Holders of Prepaid Cards (Mar. 21, 2016); Interagency Policy Statement on Funding and Liquidity Risk Management, 75 FR 13656 (Mar. 22, 2010); Interagency Interpretive Guidance on Customer Identification Program Requirements, (Apr. 28, 2005); Unfair or Deceptive Acts or Practices by State-Chartered Banks (Mar. 11, 2004).

[4] This term includes, among many others, intermediate platform providers (as defined below), 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.

to or facilitates the provision of the product or service directly to the end user.[5] These arrangements enable fintech companies to provide end users with access to a range of banking products, including deposit products (*e.g.,* checking or savings accounts); payment services (*e.g.,* peer-to-peer, debit card, contactless payments, Automated Clearing House (ACH) transactions, or wire transfer capabilities); or lending products (*e.g.,* unsecured consumer or small business loans) through online and mobile applications, platforms, or digital wallets. In some of these cases, fintech companies (sometimes referred to as a ''middleware provider'' or ''intermediate platform provider'') act as intermediaries by engaging in a variety of functions, as described in detail below. For purposes of this RFI, we refer to all of these types of arrangements as ''bank-fintech arrangements.''

Bank-fintech arrangements may enable banks to leverage newer technology and offer innovative products or services to further their digitalization efforts and to meet evolving customer demands and expectations. These arrangements may also provide banks with the ability to quickly and more cost effectively deploy products or services into the market through the fintech company. In addition, these arrangements may provide banks with access to new or expanded markets, revenue sources, and customers. As discussed in more detail below, bank-fintech arrangements also may introduce potential risks through business and legal structures that increase operational complexity, unbundle traditional banking products and services (particularly payments), and increase compliance challenges. The failure of banks to manage these arrangements effectively may present consumer protection, safety and soundness, and compliance concerns.

The following sections of this RFI describe several bank-fintech arrangement structures and use cases, as well as the risks the agencies have seen manifesting and arising from these arrangements. The agencies seek public comment to build on their understanding of these arrangements, including with respect to roles, risks, costs, and revenue allocation. The agencies also seek additional information and stakeholder perspectives relevant to the implications of such arrangements, including for banks' risk management, safety and soundness, and compliance with applicable laws and regulations. The RFI is not intended to impose any obligations or define any rights, and it is not an interpretation of any statute or regulation.

Descriptions of Bank-Fintech Arrangements

The agencies have observed that bank-fintech arrangements vary significantly in structure and product and service offerings, but many commonly fall into one or more categories of facilitating deposit-taking, payment (including card issuance and digital wallet capabilities), and lending activities. Such arrangements may be effectuated either directly between banks and fintech companies or indirectly through the use of an intermediate platform provider. The agencies seek comment on these categories and the attributes of the bank-fintech arrangements described below.

Bank-Fintech Arrangements in Connection With Deposit-Taking Activities

Some non-bank fintech companies provide end users with access to deposit products and services; however, these entities are not Federally insured depository institutions (IDIs). Instead, the fintech company establishes arrangements with one or more IDIs, directly or through an intermediate platform provider, to provide end users with access to banking products and services—such as deposit accounts, debit cards, savings accounts, and other account-related services—through the fintech company's online or mobile platform.[6] Some fintech companies enter into these deposit-taking arrangements with banks to target a specific customer base, such as underserved or younger demographics. Other fintech companies incorporate such deposit-taking arrangements into much larger suites of financial and non-financial products and services and target a much broader customer base.

In arrangements between banks and fintech companies to facilitate an IDI's deposit-taking activities, fintech companies often play a critical role in maintaining a deposit and transaction system of record. These transaction records may not be reflected in the bank's core processing system. Instead, the bank's core deposit ledger may only include omnibus accounts, often titled to reflect that they are held for the benefit of (FBO) end users. The contracts governing these arrangements commonly set forth the operational responsibilities of each party, such as record-keeping and access to records, end-user on-boarding, compliance management, transaction monitoring, and complaint handling. Bank-fintech arrangements involving deposit-taking activities often involve heightened levels of operational complexity, including as it relates to reconciliations and Bank Secrecy Act (BSA) recordkeeping and compliance (*e.g.,* customer identification and due diligence, suspicious activity monitoring, and reporting and sanctions screening).

Bank-Fintech Arrangements in Connection With Payment Activities, Including Card Issuance

Banks may enter a variety of arrangements with fintech companies in connection with fund-transfer services, card issuance, contactless payments, and other payment solutions. While banks and non-banks have entered into payment-related card sponsorship arrangements for decades, the types, number, and complexity of payment-related products and services and associated arrangements between banks and fintech companies have rapidly increased in recent years.

Today, payment-related bank-fintech arrangements can vary widely and may include several different types of payment options, including debit and credit card offerings, fund-transfer services utilizing ACH transactions, wire transfers, prepaid services, and instant payments. Non-cash payments, particularly cards and ACH transactions, have increased significantly in size and volume in recent years due to innovation and the ease, convenience, accessibility, and speed of digital payments. A fintech company may enter into a card offering arrangement with a bank to provide end users with access to bank-issued, fintech-branded debit or credit cards. In some of these card offering arrangements, the partner bank directly operates and manages the cards. In others, the fintech company directly operates and manages the cards with oversight by the partner bank pursuant to a bank sponsorship agreement between the bank and fintech company. In a prepaid services arrangement, a fintech company may offer end users access to bank-operated (and, often, fintech-branded) prepaid accounts that link to end users' accounts with the fintech company. This type of structure allows end users to load and store prepaid funds and transfer such funds to others. A fintech company may also

[5] These arrangements are sometimes referred to as ''banking-as-a-service'' or ''embedded finance'' depending on the structure and parties involved in the arrangement.

[6] Fintech companies that offer these services to end users through such arrangements are sometimes referred to as ''neobanks'' or ''challenger banks.''

enter into a bank-fintech arrangement to offer ACH transactions, wire transfers, or settlement of payment services to end users. For example, a fintech company may enter into an arrangement with a bank to offer ACH services to its end users, such as sending or receiving funds via ACH transfers, which may take place through a bank sponsorship arrangement. Additionally, operators of digital platforms permitting the transmittal and exchange of funds between and among member participants [7] enter into bank-fintech arrangements to offer a range of payment options to end users of the platforms.

Under each of these arrangements, fintech companies also may provide a variety of additional services, including providing end users with personal finance and payment management tools, marketing the branded cards and payment services to end users, or assisting banks with underwriting for credit cards (sometimes using alternative data). Additionally, under each of these arrangements, banks may provide access to various services to or for end users, including card or account issuance, back-end fund-transfer and redemption operations support, access to proprietary electronic platforms, or bill payment services.

Many fintech companies enter these arrangements with banks in order to gain access to existing payment systems and card networks. In these types of structures, a bank may enter into an arrangement with the fintech company (such as a payments platform or a card processor) to ''sponsor'' the fintech company's access to one or more payment systems or card networks to facilitate the availability of specified payment options to end users in exchange for one-time and/or per-transaction fees. In this structure, operators of payment systems and card networks may permit fintech companies to conduct transactions on payment and card networks through the bank's sponsorship arrangements with the operator. Among other things, bank sponsorship may entail the partner bank agreeing with the operators of the payment and card networks to sponsor and pre-approve the proposed payment activities of the fintech company across the payment or card networks, to monitor the fintech company's operations for compliance with operator and relevant network rules, or to accept risk-of-loss liability in connection with transactions effectuated by the fintech company.

A bank that sponsors a fintech company's access to a payment system or card network for these purposes may establish an account for the fintech company at the bank for the acceptance and settlement of end-user payments, which may be effectuated in several different ways depending on the agreement between the fintech company and bank. For example, the bank may agree to open an account FBO the end users and use it to settle payment transactions. In some cases, the fintech may provide recordkeeping functions to facilitate the settlement of end-user transactions.

Several fintech companies have also entered into arrangements with banks in recent years to offer digital wallets, often in conjunction with associated payment applications (sometimes referred to as ''pay apps''). A digital wallet is a software application that permits end users to store card account or other payment credentials in encrypted or tokenized form so that end users may recall and transmit the stored credentials via a digital payment application at physical or digital points of sale. End users may rely on digital wallet functionality, used in combination with payment applications, to make in-person, contactless payments via their mobile devices (sometimes referred to as ''tap-to-pay''). Digital wallet functionalities also may assist end users in making online purchases through web and mobile applications. Some fintech companies make their digital wallets and associated payment applications available for limited use—for instance, to effectuate purchases with a single retailer or group of retailers. Others offer general use digital wallets and associated digital payment applications available to end users at a variety of participating points of sale.

In each case, fintech companies offering combined digital wallet and payment applications typically enter into arrangements with banks that issue the debit and credit cards that end users wish to include in their digital wallets. Many of the arrangements reflect standard terms governed by the payment systems and card networks. Other arrangements may require debit and credit card issuers to pay fintech companies per-transaction fees associated with the end users' reliance on the combined digital wallet and payment applications of the fintech companies.

Bank-Fintech Arrangements in Connection With Consumer and Small Business Lending

Bank-fintech arrangements can also facilitate loans through a fintech company's online platform. Fintech companies may market and distribute a variety of loan products, including those targeted to consumers, students, and small businesses.[8] Banks increasingly engage with fintech companies to access these lending markets. The parties to these arrangements in turn may be assigned to perform various core operational functions in connection with lending, including those relating to the processing, underwriting, closing, delivering, or servicing of loans.

In a typical arrangement, a partner bank agrees to facilitate and fund loans, while the fintech company solicits end users and collects application data. In some arrangements, end-user application data collected by the fintech company is used in the underwriting process within the parameters of underwriting standards agreed upon with the bank. Loans might be retained on the bank's balance sheet, or the loans (or a portion of the loans or an interest in the loan payment streams) might be sold to the fintech company. The fintech company may then securitize any acquired loans for subsequent re-sale into the public or private asset-backed securities markets, although the bank may retain an economic interest in the performance of the loans through a variety of contractual mechanisms. The fintech company or a fourth party often performs loan servicing and collection under these arrangements.

The Role of Intermediate Platform Providers

The growth of bank-fintech arrangements has spurred the development of a new business model whereby some fintech companies provide an intermediate technology platform—sometimes referred to as an ''aggregation layer''—to facilitate relationships between banks and other fintech companies that seek to distribute banking products and services directly

[7] These platforms are sometimes referred to as ''Peer-2-Peer,'' ''Business-2-Consumer,'' or ''Business-2-Business'' platforms.

[8] Such products may also include ''buy now, pay later'' (BNPL) lending, to the extent offered through a bank-fintech arrangement; however, BNPL offerings have to date typically been offered and distributed solely through either a bank, fintech company, or consumer retailer, rather than through a bank-fintech arrangement. BNPL generally refers to point-of-sale installment loans offered to end users that are payable in four or fewer installments, often concurrently with their purchase of non-financial goods and services. For additional information on BNPL, and the risks it may pose to banks, see *Retail Lending: Risk Management of 'Buy Now, Pay Later' Lending,* OCC Bulletin 2023–37 (Dec. 6, 2023).

to end users. These intermediate platform providers enable individual banks to connect to numerous fintech companies and serve the role of introducing banks and fintech companies seeking such relationships. Intermediate platform providers may also market these services together as an ''all-in-one'' solution for fintech companies and banks by providing technological, operational, and information services in one place, enabling fintech companies and banks to connect more seamlessly. An intermediate platform provider may also offer to assist fintech companies in implementing compliance risk management programs and in handling the transfer and flow of funds across deposit-taking, payments, card issuance, or lending activities.

Operators of intermediate platforms may enter into their own arrangements with banks and third parties to provide these services. These arrangements may involve a bank providing an intermediate platform provider with permission to transfer data via, for example, application programming interfaces (APIs). A single intermediate platform provider may have arrangements with multiple banks to provide such access or provide services to banks relating to operational, compliance, data, or other functions in connection with the banks' relationships with fintech companies or the platform provider itself.

Risk Implications

While bank-fintech arrangements may offer banks significant benefits, they also may present the full spectrum of risks facing banks, including, but not limited to, third-party, credit, liquidity, compliance, and operational risk. Risks may also be heightened where the fintech is the distributor of the banking product or service to the end user, or where the fintech or intermediate platform provider performs key functions, such as handling end-user complaints, performing customer identification and due diligence, developing and transmitting disclosures, monitoring transactions, maintaining end-user ledgers, performing certain lending-related activities, developing and deploying marketing materials, or directly communicating with end users.[9] Bank-fintech arrangements may also involve a wide range of practices to deliver banking products and services to end users through a combination of the fintech company's technological capabilities and the bank's infrastructure, including the ability to provide access to deposit accounts, access to payment rails, and extend credit. These facets of bank-fintech arrangements may create heightened or novel risks for banks relative to the risks associated with more traditional third-party vendor relationships. The following discussion of risks in bank-fintech arrangements is meant to be illustrative of certain select concerns and is not meant to be comprehensive.

Accountability

Contractual accountability for different aspects of the end-user relationship may be allocated among the parties to a bank-fintech arrangement. However, banks remain responsible for compliance with applicable law. Failure to conduct sufficient due diligence, ongoing monitoring, and oversight of the bank-fintech arrangement may complicate the bank's ability to ensure such compliance and to identify risk. In addition, contractual division of labor may complicate the bank's ability to establish clear lines of accountability, implement effective risk and compliance management strategies, and address and remediate issues as they arise, especially where novel arrangements place certain traditional banking activities outside of the bank. These factors may expose the bank to compliance, litigation, and other risks.

For example, in a bank-fintech arrangement, the fintech company may maintain the end-user relationship, including by interacting directly with end users, responding to inquiries and complaints, and providing required consumer protection and other disclosures. However, independent of contractual responsibilities, the end user may still qualify as a customer of the bank for certain regulatory purposes.[10] The bank also remains responsible for its various other compliance requirements, such as Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) compliance program requirements.[11] Similarly, the fintech company's role in providing disclosures may increase the risk of inaccurate or misleading representations concerning, for example, the applicability, nature, or scope of Federal deposit insurance available to end users.[12] Such risks may be heightened where the fintech company controls the end-user relationship and uses the bank's name and branding in marketing or when an intermediate platform provider is used and further distances the bank from the end user.

Under certain bank-fintech arrangements, it may be difficult for the bank to perform oversight and control functions over the fintech company effectively where the fintech company has substantial negotiating power relative to the bank or where the bank relies on revenue or liquidity from the fintech company. Difficulty in performing this oversight and control function in turn could impede bank staff's ability to provide effective challenge to critical aspects of the bank-fintech relationship, including whether to terminate the contractual arrangement if necessary. These risks may be heightened where the fintech company is not familiar with or has a different risk tolerance concerning the specific requirements of the laws and regulations applicable to it,[13] the bank, or the products and services offered via the arrangement. These risks may be further heightened where an intermediate platform provider assists the fintech company in implementing risk management programs, such as compliance.

[9] A fintech company may also use subcontractors (referred to variously as ''nth-party risk,'' ''nested risk,'' or ''banking services supply chain risk'') in providing these services. Ineffectual oversight of subcontractors (including failure to properly account for subcontractors in the arrangement's business continuity plan) could result in material disruptions of the arrangement. *See generally* Interagency Guidance on Third-Party Relationships: Risk Management, 88 FR 37920 (Jun. 9, 2023).

[10] *See, e.g.,* 12 CFR 1016.3(i) (defining customer relationships for purposes of the Consumer Financial Protection Bureau's (CFPB) Regulation P); OCC (12 CFR part 30, App. B (I)(C)(2)(d); Board (12 CFR part 208, App. D–2 § I.C.2.d) FDIC (12 CFR part 364, App. B § I.C.2.d) (adopting Regulation P's definition of ''customer'' for the Interagency Guidelines Establishing Information Security Standards); 31 CFR 1020.100(b) (defining customer relationships for purposes of a bank's customer identification program).

[11] *See, e.g.,* suspicious activity reporting and BSA/AML program requirements for the OCC (12 CFR 21.11 and 21.21), Board (12 CFR 208.62 and 208.63), and FDIC (12 CFR 326.8 and part 353).

[12] *See, e.g.,* 12 U.S.C. 1828(a)(4); 12 CFR part 328, subpart B; FDIC, FIL–35–2022, ''Advisory to FDIC-Insured Institutions Regarding Deposit Insurance and Dealings with Crypto Companies'' (Jul. 29, 2022); *see also* 12 CFR 7.5010 (requiring banking organizations to distinguish products and services offered by it from those of a third party on co-branded websites and other shared electronic spaces). Even when the parties intend that the financial products or services will benefit from deposit insurance, application of Federal deposit insurance may be complicated in novel arrangements; 12 CFR 330.5, 330.7 (describing requirements for pass-through deposit insurance).

[13] The CFPB (for instance) possesses authority under 12 U.S.C. 5514 to engage in risk-based supervision of non-depository financial institutions participating in certain markets for consumer financial products and services. Fintech companies that are regulated as money services businesses are also subject to certain BSA/AML and state law requirements. *See, e.g.,* 31 CFR part 1022.

End-User Confusion

The fintech company's efforts to provide a seamless end-user experience could make it difficult for end users to know in what capacity they are dealing with the bank or the fintech company. In some cases, marketing materials or other statements by the fintech company or bank may exacerbate end-user confusion. For example, end users may not be well-informed regarding the type of account relationship that the end user is establishing through the fintech and may not understand that Federal deposit insurance does not protect them from a nonbank fintech company's failure. End-user confusion may also complicate compliance efforts and pose other risks to the bank. For example, an end user that is unaware of the bank's presence in the arrangement may direct complaints solely to the fintech company. The bank's ability to comply with its obligations under Federal consumer financial protection laws could be undermined if the fintech company fails to timely communicate to, or coordinate with, the bank on responses to consumer complaints.[14]

Rapid Growth

A bank may experience rapid growth as a result of engaging in a bank-fintech arrangement (*e.g.,* growth in deposits or transaction volume), especially in the case of a community bank. Various risks can emerge from rapid growth and the bank's changing risk profile, including risks that may threaten the bank's safety and soundness or its ability to comply with applicable laws and regulations.[15] These risks may arise from challenges such as appropriately scaling risk and compliance management systems, operational complexities, significant deposit growth, and insufficient capital to support the rapid growth, among other things.

For example, a bank's existing risk and compliance management systems, as well as management's and employees' expertise and roles and responsibilities, may neither be commensurate with the risk profile of the new business model nor be sufficiently scalable without significant investments in resources and training. Failure to scale compliance and risk management functions and resources with the growth resulting from the bank-fintech arrangement may increase the likelihood of the bank violating applicable laws and regulations, including those related to AML/CFT or sanctions, consumer protection, and fair lending.

Bank-fintech arrangements may also pose operational complexities, which may lead to increased risk. For example, potentially significant increases in the volume of payment processing may give rise to increased transaction monitoring alerts. In addition, depending on the integration of the bank's information technology systems with those of the fintech company, security vulnerabilities and other sources of operational disruption may arise, increasing the likelihood of data breaches, privacy incidents, service interruptions, and fraud.[16] In some cases, banks do not have or are unable to develop the infrastructure to adequately address these complexities, and instead rely on manual workarounds, which could lead to operational breakdowns that may implicate various other risks, including compliance and legal risks. These risks may be heightened where the bank-fintech arrangement involves an additional entity (*e.g.,* an intermediate platform provider).[17]

Rapid deposit growth related to a bank-fintech arrangement can also pose risks related to funds management. For example, a bank may need to invest an influx of short-term deposits that greatly exceed amounts the bank has traditionally managed. To the extent that deposits are used to fund growth in longer-term or higher-risk fixed-rate assets, including loans and securities, the bank may be exposed to greater liquidity, interest rate, or credit risk, especially when such investments are concentrated, or the risks are otherwise correlated. The bank may also experience increased liquidity stress should it need to meet material short-term withdrawal requests. Rapid deposit or asset growth also implicates various other risks, including those relating to maintaining sufficient capital to support expansion of the bank's business.[18]

Concentration and Liquidity Management

Bank-fintech arrangements may also result in the bank's business becoming highly concentrated in the arrangement. This concentration risk may amplify other risks to the bank, including from any market stresses or if deposits are used to fund longer-term assets. For example, in a rising interest rate environment, a bank-fintech arrangement involving loan products may see a reduction in originations. This reduction may pose particular risk to a bank whose business has become heavily concentrated in that arrangement and that, as a result, relies on those originations for a material portion of its earnings. Such an environment may increase the bank's exposure to credit risk from the arrangement (*e.g.,* the credit risk of the fintech company or of loans originated under the arrangement, whether still on the bank's balance sheet or for which the bank retains any contractual interest, even if repurchased by the fintech company). Such an environment may also lead to an increase in the credit risk of a bank's overall retail loan portfolio.[19]

Bank-fintech arrangements may also pose liquidity risks if the bank fails to establish adequate liquidity contingency plans and exit strategies, particularly when arrangements represent a funding concentration. An arrangement may be terminated or reduced in amount for any number of reasons, including those over which the bank has little control, and which may result in significant stress on a bank. For example, if the fintech partner or an intermediate platform provider in a deposit-taking bank-fintech arrangement faces a stress event or terminates the contractual arrangement, that could lead to a large withdrawal of end-user-related deposits, resulting in liquidity stress and losses for the bank. Failure to establish adequate liquidity contingency plans and exit strategies could also increase operational and strategic risks for the bank.

[14] For example, the bank's ability to comply with its dispute and error resolution obligations or undertake its risk monitoring capabilities could be impaired.

[15] *See* OCC Bulletin 2017–43, *New, Modified, or Expanded Bank Products and Services: Risk Management Principles* (Oct. 20, 2017) for a general discussion of these risks.

[16] Integration could also introduce security vulnerabilities, including by providing another access point into the bank's systems. Integration may amplify operational risks, such as fraud, cybersecurity, and data privacy incidents occurring at the fintech company that then affect the bank.

[17] The growing prevalence of nested relationships may materially alter the traditional third-party risks present, complicating the bank's ability to provide effective oversight to the arrangement. This is especially so if the additional entity may be contractually allowed to add operating partners or subcontractors without the bank's prior consent. *See* ''Interagency Guidance on Third-Party Relationships,'' *supra* note 9, for more.

[18] Additionally, to the extent that a fintech company meets the definition of a deposit broker under 12 CFR 337.6, any related deposits would be brokered deposits subject to applicable restrictions if the bank becomes less than well capitalized under the prompt corrective action provisions of the agencies' capital rules.

[19] These risks may be heightened where the arrangement results in the bank's risk profile becoming more correlated to or concentrated in a particular market segment or asset type, either directly through its exposure to certain products, or indirectly through its exposure to the fintech company.

Use and Ownership of Data and Customer Information

Bank-fintech arrangements often rely on new, innovative, and potentially untested uses of data to expand or enhance access to financial services, which may in turn lead to risks related to compliance with laws and regulations, operational challenges, and the ownership, use, and nature of that data. For instance, a bank-fintech arrangement may be premised on underwriting credit using alternative data. Introducing alternative data into a bank's existing systems may pose risks. These include, for example, risks related to the bank's ability to address concerns associated with alternative data and its use (including as to accuracy and biases) and to incorporate alternative data types and formats into its information technology systems, credit risk modeling capabilities, and compliance management systems.[20]

Data ownership and use questions may also create risks for the bank. For instance, the fintech company may attempt to limit the bank's access to data generated as part of the arrangement if the fintech company views the data as its proprietary information. Other issues related to data ownership and use may arise where banks are required by law to limit the fintech company's access to and use of certain data. For example, banks are restricted in the sharing, use, and disposal of end user nonpublic information, and end users may have opt-out rights, which could pose operational difficulties and compliance risks.[21] Therefore, the bank may require information on the bank-fintech arrangement's end users to meet its own compliance obligations, including, but not limited to, those related to recordkeeping, AML/CFT or sanctions, fair lending, or state escheatment statutes or regulations. This requirement for information may arise even where the bank lacks a direct relationship with end users or where they are not named account holders with the bank.[22] As discussed in more detail above, these risks may be heightened where aspects of the end-user relationship or compliance-related activities are contractually allocated among multiple entities (*e.g.,* intermediate platform providers).

Request for Comment

In this RFI, the agencies are inviting interested members of the public to comment on the descriptions of bank-fintech arrangements and risks summarized in the document. The agencies are also seeking comment on effective practices for managing these risks. Where questions ask for the ''range of practices,'' respondents are encouraged to describe the practices' advantages and disadvantages.

Bank-Fintech Arrangement Descriptions

1. Do the descriptions and categorizations in this RFI adequately describe the types of bank-fintech arrangements in the industry and the companies involved? If not, why? Are the descriptions or categorizations overly broad or narrow, or are there any types of companies or categories of arrangements missing from the descriptions?

2. Are there any benefits of bank-fintech arrangements that are not addressed by this RFI? What benefits do the bank or the fintech company receive by using an intermediate platform provider?

3. Describe the range of practices regarding banks' use of data [23] to monitor risk, ensure compliance with regulatory responsibilities and obligations, or otherwise manage bank-fintech arrangements. What data and information do banks typically receive in bank-fintech arrangements, including in those involving intermediate platform providers? To what extent is this information different from the information banks would receive when interacting with end users independent of fintech companies? What challenges have banks experienced in bank-fintech arrangements—including those involving intermediate platform providers—related to the timely access to customer information, and what steps have the parties to bank-fintech arrangements taken to assess potential compliance issues associated with such challenges?

4. How do the parties to bank-fintech arrangements determine the end user's status as a customer of the bank, the fintech company, or both, including for purposes of compliance with applicable laws and regulations, and each party's responsibility in complying with contractual requirements? What disputes or uncertainties regarding the status of end users have the parties experienced, and how have they sought to resolve them? How does the type of arrangement impact such determinations?

5. Describe the range of practices regarding the use of a core bank service provider or other third-party providers in bank-fintech arrangements. How do these providers help or hinder bank-fintech arrangements?

6. Describe the range of practices in cases where bank-fintech arrangements involve affiliates of the bank, including fintechs. What are the benefits and risks of these arrangements?

7. Bank-fintech arrangements can involve significant up-front and ongoing costs and resources for the bank involved and may take some time to recoup these costs and resources. What type of up-front and ongoing costs and resources are associated with establishing bank-fintech arrangements? Describe the range of practices regarding how a bank factors such upfront costs and resources into its overall strategy and risk management strategy. Describe the range of practices regarding how revenues and costs resulting from these arrangements are allocated between the bank and fintech company.

Risk and Risk Management

1. Describe the range of practices for maintaining safety and soundness, and compliance with applicable laws and regulations arising from bank-fintech arrangements. How do the practices differ as between different categories of arrangements? Does the RFI adequately identify and describe the potential risks of bank-fintech arrangements?

2. Bank-fintech arrangements can present unique or heightened consumer protection risks, such as risks of discrimination, unfair or deceptive acts or practices under the Federal Trade Commission Act, or privacy concerns. Describe the range of practices for managing any heightened risks.

3. Describe the range of practices parties to a bank-fintech arrangement may use in contractually allocating functions among themselves, including the advantages and disadvantages of each such practice. For example, while the parties to such arrangements remain responsible for their own compliance with applicable laws and regulations, as a matter of contractual allocation, who performs which activities related to risk and compliance management, customer identification and due diligence,

[20] For example, alternative datasets that impact credit decisions could potentially create or heighten consumer protection risks, such as unlawful discrimination in lending.

[21] *See* Title V, subtitle A of the Gramm-Leach Bliley Act, Public Law 106–102, 113 Stat. 1338, codified in relevant part at 15 U.S.C. 6801 *et seq.,* implemented at OCC (12 CFR part 30 Appendix B, including Supplement A), Board (12 CFR part 208 Appendix D–2, including Supplement A), FDIC (12 CFR part 364 (Appendix B, including Supplement A), and 12 CFR part 1016 (Regulation P).

[22] *See, e.g.,* suspicious activity reporting and BSA/AML program requirements for the OCC (12 CFR 21.11 and 21.21), Board (12 CFR 208.62 and 208.63), and FDIC (12 CFR 326.8 and part 353). *See also supra* note 10 and accompanying text.

[23] For example, key performance indicators, product-level data, service levels, end-user information, key risk indicators, consumer complaints, fraud monitoring metrics, or KYC/CIP information.

transaction monitoring, sanctions screening, fraud monitoring, end-user complaint management, dispute resolution, data protection, or credit underwriting, if applicable? Who develops and oversees marketing materials, develops and provides disclosures and account statements, addresses errors, receives and resolves disputes, and responds to complaints? How are contractual breaches and indemnifications typically addressed in these types of arrangements? Describe the range of practices for monitoring compliance with applicable laws and regulations, notwithstanding contractual allocations.

4. How are risks resulting from these arrangements, including those concerning credit, liquidity, concentration, compliance, and operational risk, as well as concerns regarding negative end-user experience managed? What techniques or strategies are most effective in managing the impact of rapid growth, particularly related to deposit-taking and payment-related arrangements?

5. Describe the range of risk management strategies banks and fintech companies use to ensure that required disclosures in bank-fintech arrangements, including those relating to rates and fees associated with end-user banking products and services, are accurately and plainly communicated, and comply with all relevant state and Federal laws and regulations.

6. Describe the range of practices regarding disclosures (*e.g.,* initial, annual, or ongoing) to end users about the involvement of bank-fintech arrangements in the delivery of banking products and service.

7. Describe the range of practices regarding the use of an intermediate platform provider. Describe how the use of an intermediate platform provider may amplify or mitigate risk, and to what extent, if any, intermediate platform providers influence how banks handle operational, compliance, or other issues when dealing with fintech companies within the intermediate platform provider's network.

8. Describe the range of practices regarding how banks manage the risks of connecting to multiple technology platforms and exchanging data in bank-fintech arrangements.

9. Describe the range of practices regarding planning for when a fintech company or intermediate platform provider exits an arrangement, faces a stress event, or experiences a significant operational disruption, such as a cyber-attack. Describe the range of practices regarding how arrangements are structured to minimize harm to end users, meet compliance requirements, and minimize liquidity risks and other risks in the event of such exits, stresses, or disruptions.

10. Describe the range of practices, and challenges, in negotiating contracts with, or conducting due diligence on fintech companies. Describe the range of practices in maintaining ongoing monitoring of bank-fintech arrangements, particularly related to risk management, regulatory compliance, data ownership and use, and information security assessment rights. What impact, if any, does the size and negotiating power of the bank or the fintech company have on these issues? What impact, if any, does the fintech company's or intermediary platform provider's degree of control of operational functions have on these issues? What impact, if any, does bank liquidity or revenues concentration represented by any particular fintech company, intermediary platform provider, or business line have on these issues?

11. Bank-fintech arrangements may involve processing payments transactions unrelated to any specific deposit-taking or credit offering in significant volumes. Describe the range of practices that banks adopt to manage potential risks associated with processing large volumes of otherwise unaffiliated payments transactions. Do banks view bank-fintech arrangements involving such processing differently from other payments-related products and services offered to end users?

12. How do banks ensure bank-fintech arrangements can be suspended or terminated based upon safety and soundness, compliance, or consumer protection concerns? What fees or other costs are typically involved in exiting these arrangements?

13. Are there other techniques or strategies that banks use to manage the various risks bank-fintech arrangements may present? Which of these techniques or strategies are most effective in managing such risks?

14. In the context of bank-fintech arrangements, how are deposit accounts usually titled? Describe the range of practices reconciling bank deposit account records with the fintechs' records. Generally, what party holds and maintains the account records? Describe the structure in place to exchange accurate customer information between the bank and the fintech company and how the agreements between banks and fintech companies generally address these matters. Describe any additional controls, that banks or fintechs may use to provide for accurate reconciliations.

15. Describe the range of practices regarding the maintenance of systems of records and account titling in the context of bank-fintech arrangements. Do certain account structures pose greater risk considerations to banks and end users than others? What additional controls, if any, do banks or fintechs place on these accounts to manage these risks?

16. To what extent would additional clarifications or further guidance be helpful to banks with respect to bank-fintech arrangements? If so, please explain. In what specific areas would additional clarification or further guidance be most helpful?

Trends and Financial Stability

1. What data would be helpful for the agencies in monitoring developments regarding bank-fintech arrangements? For example, this might include data to assist in monitoring developments and trends in bank-fintech arrangement structures and use cases, concentrations, and the number and types of bank-fintech arrangements in the financial services industry.

2. In what ways do or can bank-fintech arrangements support increased access to financial products and services? Alternatively, in what ways do or can these arrangements disadvantage end users?

3. In what ways might bank-fintech arrangements function as transmission mechanisms to amplify financial shocks (*i.e.,* threaten financial stability)? Conversely, how could these arrangements help to contain shocks and reduce contagion?

4. What factors are important in determining whether bank-fintech arrangements support or hinder responsible innovation and a competitive and compliant financial services landscape?

Michael J. Hsu,

Acting Comptroller of the Currency.

By order of the Board of Governors of the Federal Reserve System.

Ann E. Misback,

Secretary of the Board.

Federal Deposit Insurance Corporation.

Dated at Washington, DC, on July 23, 2024.

James P. Sheesley,

Assistant Executive Secretary.

[FR Doc. 2024–16838 Filed 7–30–24; 8:45 am]

BILLING CODE 4810–33–P; 6210–01–P; 6714–01–P