stripe

October 30, 2024

Via eRulemaking Portal; regs.comments@federalreserve.gov; comments@fdic.gov

Chief Counsel's Office, Attention: Comment Processing
Office of the Comptroller of the Currency, Treasury
Docket No. OCC-2024-0014

Federal Reserve Board of Governors
Attn: Ann E. Misback, Secretary of the Board
Docket No. OP-1836

James P. Sheesley, Assistant Executive Secretary
Federal Deposit Insurance Corporation
RIN 3064-ZA43

Ladies and Gentlemen:

Re: Request for Information (RFI) on Bank-Fintech Arrangements Involving Banking Products and Services Distributed to Consumers and Businesses

Stripe appreciates the opportunity to provide a response to the interagency RFI seeking information about bank-fintech arrangements.

Stripe is a technology company that partners with banks to provide a range of products and services to businesses, nonprofits and others operating on the internet. Our users include businesses of every size, from small start-ups to large public companies. In 2023, Stripe processed $1 trillion in payment volume, equivalent to 1% of the global GDP.

We believe that now is an appropriate time to evaluate the bank-partnership arrangements that are aimed at developing new financial and nonfinancial products and services as well as new means of delivering such products and services. Most important in that effort is the deep examination of the risks presented by these arrangements; that examination is critical to informing and shaping proportionate (i.e., risk-based) regulation and supervision. As stated in public testimony we gave earlier this year to the House Financial Services Subcommittee on Financial Inclusion and Monetary Policy,[1] we recommend the support of bank-fintech partnerships and urge regulators to push more nuance into the supervisory process. This letter, which is grounded in Stripe's experiences with bank partnerships over more than a decade, seeks to advance that effort.

[1] Testimony of Amy Roberti, Stripe Public Policy, at the July 12, 2024 Hearing of House Financial Services Subcommittee on Financial Inclusion and Monetary Policy on "Financial Institution-Fintech Partnerships: Leveraging Third-Party Relationships to Increase Access to Financial Services."

The letter sets forth Stripe's responses to the RFI as follows:

I. General responses to the RFI's description of bank-fintech arrangements and their purposes
II. Detailed descriptions of Stripe products and bank partnerships, including function allocation, data disclosure, and relationships with the user/business customer
III. Overview of Stripe's risk and compliance management processes
IV. Stripe's suggestion regarding supervisory guidance and commentary on the recently proposed federal regulatory framework for payments

For ease of use, we have included a table (located at the end of this letter) that indicates the paragraphs where our responses to the specific RFI questions can be found.

I. Overview of bank-fintech arrangements

1. **Overall, the RFI has good broad coverage of existing bank-fintech arrangements and provides accurate descriptions of the types of arrangements that exist today.** Although the RFI acknowledges that these arrangements enable both banks and fintechs to offer more customers a broader range of products and services, the RFI is centered on the increased "access to banking products and services." The RFI's list of "banking products" include payment services with the examples being "peer-to-peer, debit card, contactless payments, Automated Clearing House (ACH) transactions, or wire transfer capabilities" (RFI p.9). The inclusion of peer-to-peer and contactless payments in a list of banking products is a particular viewpoint that de-emphasizes the role of nonbanks in developing new products. It is important to recognize that fintechs do offer financial services as the primary provider with the bank partners participating as service-providers to the fintechs.

2. **The RFI identifies potential new risks introduced by bank-fintech arrangements but does not recognize the potential of those arrangements to reduce or eliminate risks that banks and their customers face today and to improve banks' operations and products**. On their own, most banks offer a traditional suite of financial products (sometimes online) and rely on legacy systems. Perhaps the primary reason for banks' partnering with fintechs in the offering of banking products is the fintechs' integrated software and technology platforms. That platform enables faster, more cost-effective, better products and improves connections both for a bank's internal operations and between banks and their service providers (including fintechs). The legacy systems carry risks - in particular, operational risks but also legal, reputational, regulatory, and credit risks. The partnering of banks with fintechs provides benefits of automation (reducing reliance on manual operations and the instances of human error), data ingestion, and powerful processing to enable more secure and more reliable systems for data processing, money movement and storage; improved data analysis for more nuanced and accurate risk assessments, including user credit risk; as well as speedier, more efficient, and less costly delivery of financial services to end customers. In addition, technology can help banks to detect and reduce fraud, better understand potential new customers (thus expanding their reach and reducing the risk of exclusion), and improve credit scoring.

3. **The RFI uses the term "fintech" to capture all types and sizes of nonbank firms yet this agglomeration risks muddying the water for supervisors.** Some fintechs operate as licensed money transmitters, subject to regulation and supervision by the regulator(s) issuing the license(s). Other fintechs engage in lending and/or licensed loan brokering and servicing. The different fintechs' activities and the related risks and applicable regulatory requirements vary (as do the roles of the different fintechs vis-a-vis their partner banks). These various types of fintechs partner with banks in two distinct ways: the fintech may be offering its own services to the customers with the bank providing a service to the fintech; or the fintech may be operating as the customer interface to deliver services of and for the bank. The risks will generally be more circumscribed when the fintech is offering its own products and the bank is acting as the fintech's service provider.

4. **There is no model arrangement but there are certain functions that are often the contractual responsibility of the fintech (even if often the bank is required, by regulation, to comply and has engaged a fintech or other third party to perform the function).** In most of Stripe's arrangements, Stripe would be responsible for a Customer Identification Program (**CIP**) and know-your-customer/customer due diligence (**KYC/CDD**) controls applied at onboarding, account creation, and ongoing monitoring. Stripe is also typically responsible for transaction monitoring although banks will likely still engage in transaction monitoring as they will have additional views of the parties to transactions. Both Stripe and the partner bank are responsible for their individual compliance with sanctions programs. Set forth in paragraph 6 below are the functions that typically are Stripe's responsibility in its bank partnerships. Additional responsibilities with respect to specific products are noted in subsequent paragraphs.

5. **The two parties to the arrangement may both have contractual relationships with the user (business) although for some products, the business has only a contractual relationship with the fintech or the bank.** In some cases, the user is not a customer of the bank until a threshold is passed (e.g., users of Stripe's payment card-acquiring API become customers of a sponsor bank after passing the $1 million threshold for card-based transactions). And in some cases, the user may be a customer of the bank but not for purposes of the specific product or service.

II. Specific arrangements as illustrated by Stripe products and bank partnerships

6. **Common allocation of responsibilities and functions**. When a product is offered in partnership with one or more banks, Stripe is often contractually responsible for a number of functions including the following:

    a. CIP and KYC/CDD controls;

    b. transaction monitoring and reporting to the bank partner to resolve downstream issues; the partner bank may also conduct transaction monitoring (but not, for

example, for Stripe's card-acquiring business described in paragraphs 11-12 below);

c. compliance with sanctions programs;

d. fraud monitoring at the time of onboarding and during transaction processing; the partner bank may conduct additional fraud monitoring;

e. complaint management with respect to Stripe's users and, when necessary, escalating issues to bank partners or requesting additional transaction information needed from bank partners;

f. administration and resolution of Stripe merchant user dispute and error resolution;

g. protecting user data (as the bank must do as well) and confidential information of the bank (and the bank has the reciprocal obligation with respect to confidential information of Stripe).

Some of the product descriptions in paragraphs 8-19 below list additional functions for which Stripe is responsible.

7. **Data Sharing by Stripe and partner banks depends on the product.** For example, for Stripe's ACH Direct Debits product (where merchants can collect debit payments from their customers with U.S. bank accounts for charges related to the sale of goods or services), Stripe provides its partner banks (which originate the ACH transactions initiated by merchants and settle funds to the merchant's account) with both customer- and merchant-collected data for each ACH transaction. Customer-collected fields include routing number, account number, account type (checking, saving), individual name or receiving or company name. Merchant-collected fields include merchant or company name, statement descriptor (selected by merchant, frequently a derivative merchant name), values which Stripe translates into SEC [Standard Entry Class] Code, internal transaction reference token (randomly generated unique ID for a particular transaction), and transaction amount. Stripe also shares transaction failure or dispute reason; banks share transaction failure or dispute reason (if applicable) with Stripe. For Stripe Capital (see paragraphs 13-15 for more detail), Stripe provides bank partners on a daily basis (and sometimes multiple times per day) with a merchant's payment processing volume data, identifying information, application information, platform transaction data (if applicable), and underwriting information from credit decisioning.

A. Stripe payments products:

8. **Stripe's technology and tools enable our users to more easily, quickly, and safely accept payments.** In 2023, Stripe processed $1 trillion in payment volume, equivalent to 1% of the global GDP. These payments may be coming from almost anywhere in the world and not only through credit and debit cards and over ACH rails: there are over 600 different payment methods. Enabling the acquisition of large numbers of payments every second arriving from hundreds of different sources is primarily a software challenge.

9. **Stripe's ACH Direct Debit allows merchants to collect debit payments from their customers with U.S. bank accounts for single or recurring charges related to the sale of goods or services.** This product is a lower-cost option for payment collection for merchants than cards, allowing them to "pull" funds directly from a customer's bank account using the banking details a customer provides at checkout. Stripe also conducts customer bank account validation in accordance with National Automated Clearing House Association (**Nacha**) rules and provides faster settlement of funds for certain eligible merchants.

10. **The ACH Direct Debit Stripe-bank partnership arrangements are as follows**:
    a. To offer ACH Direct Debit, Stripe partners with banks to gain access to the Nacha-governed direct debit rails. (The banks are the Originating Depository Financial Institutions (**ODFIs**) that originate ACH transactions initiated by merchants and ultimately settle funds to a merchant's account. Nacha rules require ODFIs to be depository institutions in order to originate a debit transaction.)

    b. Stripe is contractually responsible for the functions noted in paragraph 6 above as well as the following:

        i. developing and maintaining a Customer Identification Program (**CIP**) delivered through KYC/CCD controls applied at onboarding, account creation and through ongoing monitoring;

        ii. establishing a credit risk policy that includes underwriting new users, credit reviews for account capability requests (e.g. faster settlement), periodic credit reviews, and ongoing monitoring. Policies are shared with partner banks for informational purposes;

        iii. production and marketing of ACH Direct Debit marketing materials.

    c. Regarding data protection:

        i. Bank partners require that Stripe comply with laws in all jurisdictions concerning data protection, bank secrecy, privacy of personal and other data related to transactions and interactions with third parties, and as needed to permit processing, including under Nacha rules.

        ii. The Nacha Rules and Guidelines set forth ACH Data Security requirements for ACH participants engaged in ACH Processing, requiring protection of sensitive data and access controls, self-assessment, and verification of identity of originators (i.e., Stripe merchants) by way of commercially reasonable systems and standards, citing sources such as FFIEC Info Security standards, NIST Cybersecurity Framework, and FTC Storage guidance as appropriate guidelines. Stripe is a Third Party Sender under the Nacha Rules and acts as a third party service provider helping Stripe users originate transactions with their end customers on their behalf.

iii. Nacha guidelines are enforced through audits and ongoing assessments as necessary.

11. **Stripe's card-acquiring business is a set of simple application programming interfaces (APIs) and software services that enable merchants and platform customers to integrate payments acceptance functionality into their websites or applications.** The APIs contain the functionality to process card transactions (including charges and refunds), make transfers to a merchant's bank account, manage customers (which includes vaulting credit card information in a PCI-compliant infrastructure), and the ability to set up and control subscription billing, all securely and promptly. The banks provide sponsored membership with the card networks (as only depository institutions may be acquirers under the card network rules in the United States) and their involvement is disclosed to Stripe users in Stripe's terms of service and at stripe.com/legal. Stripe users that process more than $1 million in transactions on a card network in a given year become automatically bound by the sponsor bank acquirer terms that are listed on Stripe's website.

12. **The RFI description of this type of card-acquiring arrangement refers to the partner bank's agreement to acceptance of risk of loss in connection with transactions effectuated by the fintech.** In Stripe's partnership with banks, Stripe is responsible for all losses related to merchant card acquiring. Only if Stripe fails would the partner bank be exposed to those losses.

B. Stripe Credit Products:

13. **Stripe offers a suite of financing products ("*Capital*") that provide small businesses with access to financing early in the company life-cycle, helping them grow.** The Stripe Capital application is a streamlined, online experience, which results in timely loan application review and funds disbursal, often occurring within a few days of loan application submission. Stripe Capital financing is repaid through withholding of funds received by Stripe in payment processing, and small businesses do not have to take extra steps to repay their loan. Stripe Capital does not impose onerous personal guarantees or other features of traditional lending products that create risk of harm to small business owners. Stripe platform users also engage in limited promotional activities related to Stripe Capital, enabling the Stripe platform user's customers to receive access to Stripe Capital.

14. **The Stripe-bank partnership arrangements for Stripe Capital are as follows**: Stripe partners with banks to help distribute bank-originated financing to Stripe's customers, which expands the banks' reach to a new customer base. (A customer relationship between a Stripe user and the bank is established when the banks extend financing to the user. Users sign a tri-party agreement between the user as recipient of financing, a bank as originator of financing, and Stripe as a broker and servicer of loans.) The banks' involvement in the program is conspicuously disclosed throughout the application, marketing materials, the borrower agreement, and every other standardized communication, consistent with a valid "true lender" construct. This bank partnership enables Stripe to offer bank financing products in almost every state on equal terms; a

similar product offered without a bank would be subject to a patchwork of state laws and would require program adjustments that could lead to disparate treatment of customers based on different state-level legal requirements.

15. **Stripe Capital falls within the RFI description of bank-fintech arrangements in connection with consumer and small business lending, although Stripe Capital is for businesses only, not consumers.** Consistent with arrangements described in the RFI, Stripe underwrites its users pursuant to the credit policy approved by the bank partner, with Stripe data (e.g., payment processing data) being a primary data source. Stripe sells Capital loans to investors and also pledges Capital loans to secure a credit facility. While the RFI refers to fintechs (or a fourth party) undertaking loan servicing and collection, Stripe is contractually bound to perform these functions *pursuant to policies and procedures approved by the bank*. When a Stripe platform user takes on these functions and receives complaints, it must submit the complaints to Stripe for resolution in accordance with those bank-approved policies and procedures.

C. Stripe Card Issuing Products:

As the RFI describes card issuing arrangements at a high level, we have provided detail from Stripe's Issuing product that may illuminate how card programs can benefit businesses and how the various functions (including risk and compliance management, KYC, complaint management etc.) are allocated between the bank and Stripe.

16. **Stripe Issuing is a suite of commercial credit and debit card products ("*Issuing*") which enable Stripe customers to create and manage custom card programs via a Stripe Issuing API.** Stripe Issuing helps Stripe customers solve various payment challenges. From businesses seeking an employee expense card program, to on-demand delivery services needing physical or virtual cards to complete customer orders, Stripe Issuing helps businesses manage payments with the ability to implement appropriate controls (e.g., spend limits, geographic restrictions). Stripe Issuing serves customers at all stages of development, from startups to large enterprises. For Stripe platform users looking to provide customers with the ability to use business cards, Stripe Issuing enables these platforms to offer access to Stripe Issuing, or to offer its own card program through Stripe Issuing. In every case, Stripe Issuing helps manage compliance on behalf of the bank, subject to bank policies, procedures and oversight.

17. **The Stripe-bank partnership arrangements for Stripe Issuing are as follows:** Stripe relies on banks because only depository institutions can become principal members of card networks and issue network-branded cards. Stripe acts as a program manager for bank-sponsored card programs and leverages Stripe money movement capabilities to settle transactions with the issuing banks. Stripe Issuing customers are customers of both Stripe and the issuing bank. The Stripe customer has one agreement with Stripe as program manager (Stripe provides front-line customer support and communications related to the program) and a separate agreement with the bank as card issuer and, when applicable, the provider of credit.

a. Stripe is responsible for the functions listed in paragraph 6 above and the following:

i. risk and compliance management, subject to bank oversight and policies approved by bank; if a Stripe platform user offers its own card program or access through Stripe Issuing, Stripe oversees such activities and provides guidelines that the platform is required to follow;

ii. performing KYC on behalf of the bank pursuant to the bank's policies and procedures; if a Stripe platform user offers its own card program through Stripe Issuing, such platform may have independent responsibilities for customer identification and KYC, depending on the nature of the card program;

iii. complaint management (including resolution), with escalation of certain complaints to the bank partner, and has an ongoing obligation to report complaints to the bank; if a Stripe platform user operates its own card program through Stripe Issuing, such platform may resolve its own complaints and Stripe oversees the platform's complaint management;

iv. underwriting (with respect to credit programs) on behalf of the bank, subject to bank-approved credit policies; if a Stripe platform user offers its own credit-based card program through Stripe Issuing, the platform may have its own credit policy and underwriting criteria;

v. generating marketing materials pursuant to guidelines provided by the bank partner and consistent with applicable law; if a Stripe platform user offers its own card programs through Stripe Issuing, such platform may generate its own marketing materials subject to Stripe oversight;

vi. providing disclosures with the issuer of the card conspicuously disclosed on all surfaces that discuss the bank-sponsored card program.

D. Stripe Stored Value Accounts:

18. **Stripe provides stored value accounts to Stripe customers and the customers of Stripe platform users; these accounts enable customers to store and send money via wire transfer and ACH ("*Treasury*").** This type of account is described in the RFI. However, it is important to underscore that Stripe relies on its money transmission licenses (with a time-tested known regulatory system that includes a requirement akin to a safeguarding or permissible investment requirement) as opposed to an unregulated pre-paid model. Stripe customers – which are businesses, small and large (and not consumers) – use this product as an alternative to a traditional bank account, which can be burdensome for small businesses to obtain, especially those in unbanked or underbanked communities. Stripe's platform user can embed banking-as-a-service into its

platform; the platform can then provide its customers with access to Stripe Treasury accounts.The bank does not have a customer relationship with the Stripe customer.

19. **The Stripe-bank partnership arrangements for Stripe Treasury are as follows:** Stripe establishes the policy for credit underwriting to determine whether to onboard a user to the program based on Stripe's eligibility criteria. Bank partners are needed to hold and transfer funds on behalf of Stripe customers. Additionally, through a bank partnership, accounts may be eligible for FDIC "pass-through" insurance (as described in the RFI). Stripe is responsible for customer-facing FDIC disclosures. If the bank needs to present disclosures in connection with the program, the bank will provide Stripe with such disclosures and Stripe is contractually obligated to present such disclosures to Stripe customers. When marketing the program, Stripe is subject to certain permissions from and oversight by the bank partner; eligibility for FDIC "pass-through" insurance must be marketed in strict accordance with regulatory requirements. (Where Treasury is made available through a Stripe platform user, the platform is responsible for hosting the user-facing FDIC disclosures and for marketing consistent with Stripe guidelines and with oversight by Stripe.)

III. Overview of Stripe's risk and compliance management processes

The RFI seeks input on risk and risk management practices. In general, Stripe has strong risk management practices that undergo regular independent audit as well as bank partner and card network review. Our practices align with and operate within the risk appetite of our partner banks in their own risk management frameworks; we continuously review and align on those frameworks with our partners and receive regular feedback. We answer the questions broadly by describing Stripe's risk organization, how it functions, and the range of practices across our various products.

20. **Stripe's risk organization leverages a combination of heuristics, machine learning models, and manual reviews to identify risks, risk-rate Stripe's merchants, and apply controls to mitigate such risks.** Stripe applies this framework across millions of merchant accounts. Stripe is constantly improving its controls based on new data and risk trends.

21. **Stripe's underwriting and onboarding processes are designed to comply with applicable laws, card network rules, bank sponsor requirements, and financial crime standards.** Thousands of new Stripe accounts are created every day. In the background, Stripe is managing risk by collecting user data and performing checks at account application submission and account activation, and by performing continual checks through ongoing monitoring. The relevant bank sponsor similarly undertakes checks based on its own risk parameters. In the event that the bank sponsor identifies as a merchant outside of its risk parameters, Stripe and the bank sponsor follow service-level agreements for offboarding the user based upon the type of risk that the user poses. The card networks similarly review merchant processing to ensure that users meet card network rules.

22. **Stripe's risk and compliance management function is subject to overlapping oversight by our bank partners, card networks, and state and federal financial regulatory agencies through (i) routine reporting, communication, and risk alerts, (ii) sampling, (iii) audits, and (iv) examinations.**

    a. Routine Reporting, Communication, and Risk Alerts**.** Stripe and our main bank partners speak almost daily about onboarding of users, ambiguous cases, and evolving risks. Stripe and its bank partners also communicate about individual users if the bank sponsor needs more information to make a risk determination or its risk appetite has evolved. Stripe is contractually required to submit financial statements and records to bank partners on an ongoing basis. Stripe is also subject to recordkeeping requirements imposed by law. Stripe submits call reports on a quarterly basis to state financial regulators pursuant to state-level money transmitter statutory and regulatory requirements. This reporting provides regulators information about transactional activity and permissible investment amounts, and often includes information on in-state, foreign, and domestic transactions, permissible investment details, agent transaction details, and volume and dollar amount of transactions completed.Stripe also regularly submits suspicious activity reports to FinCEN, both under its regulatory obligation as a regulated money services business and, far more frequently owing to its volumes, voluntarily as a payment service provider.
    b. Sampling. Stripe is subject to regular sampling of its users by bank sponsors. This process involves a deep dive on a random set of users to ensure compliance with card network rules, contractual obligations, and regulatory requirements.
    c. Audit. Stripe is subject to regular and frequent audit and enhanced due diligence reviews through its contracts with bank partners. To conduct audits, the relevant bank partner and Stripe will meet on-site for thorough review of systems, users, and the overall risk and compliance program. Stripe and its bank partners are also subject to audit by the card networks. As a regulated money services business, Stripe also conducts an independent audit of its AML compliance function annually, both within the regulated money services business and across the broader enterprise.
    d. Examination. Stripe is subject to regular and comprehensive examination by state financial regulators as a result of its state-level money transmission licenses. Stripe is examined at least annually by multistate teams and/or individual states to ensure it operates in a safe and sound manner and adheres to state and federal laws and regulations. As a regulated money services business, Stripe is also subject to examination for compliance with federal AML laws and regulations by the Internal Revenue Service. Stripe's bank partners are also subject to regular examination by state and federal banking agencies.

IV. Stripe's suggestion regarding supervisory guidance and commentary on the recently proposed federal regulatory framework for payments

23. **Supervision and examination of third-party providers.** Under the Bank Service Company Act (**BSCA**), any third party provider of services to a bank is subject to

examination by the bank's regulator to the same extent as if the service were performed directly by the bank. Through the BSCA, federal banking agencies (**FBAs**) have developed an examination program to supervise larger and more material service providers (known as Significant Service Providers and Regional Service Providers, formerly referred to as Technology Service Providers or **TSP**). Through the FFIEC, the FBAs have set forth examination criteria, standards, guidance and handbooks to help guide examiners and service providers alike in understanding expectations and requirements. To the extent that the FBAs seek to expand use of the BSCA authority to conduct more examinations of third-party service providers to banks, including fintechs, we urge the FBAs to design and release materials similar to the FFIEC's TSP program that provides transparency into the scope of such examinations and supervision. Such transparency may help banks that utilize such service providers to understand how such service providers are examined and adjust their due diligence and oversight programs accordingly. We also believe that a transparent program will help FBAs and other supervisors calibrate the scope of such examinations consistent with the BSCA's grant of authority.

24. **Federal regulatory framework for payments.** Treasury Undersecretary Nellie Liang's recent comments on and endorsement of a federal regulatory framework for payments emphasize the importance of fintechs to competition and innovation in payment services. We believe that U.S. payments rules should advance the goals noted by the Undersecretary, namely: (1) supporting U.S. global leadership of financial firms, (2) promoting innovation and fair competition, and (3) addressing important payment services risks and infrastructure limitations. Regarding these limitations, the Undersecretary has acknowledged that money transmitters' lack of access to critical payments infrastructure and systems – including ACH and FedWire – impedes their ability to offer products and services their users want and need.

    The Undersecretary notes possible consideration of imposing affiliation and activities restrictions on payments firms and commercial activities. We agree that money transmitters and similar entities should limit their direct activities to payments and affiliated functions and not engage in credit or significant maturity transformation. However, we believe that limits on affiliations among payments companies and other commercial enterprises are unnecessary and would unduly limit innovations and synergies in the payments space.

* * * * *

Thank you for considering this letter. Should you have any questions or require any additional information, please do not hesitate to contact me at gerrytsai@stripe.com.

Respectfully submitted,

//S//

Gerald Tsai

Annex to Stripe Response to Interagency RFI

Table: RFI Questions and relevant paragraphs with responses

RFI Question		Paragraph #
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?	1, 3
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?	1, 2
3	Describe the range of practices regarding banks' use of data 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?	7
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?	9, 12, 15, 16
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?	n/a

RFI Question		Paragraph #
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?	n/a
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.	n/a
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?	1, 2, 3, 10, 11, 12,
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.	n/a
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, 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	4, 6, 9, 12, 15, 17, 19

RFI Question		Paragraph #
	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?	14, 17, 19
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.	14, 17, 19
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.	9, 14, 17, 19
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.	n/a
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.	n/a
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.	12

RFI Question		Paragraph #
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?	n/a
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?	n/a
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?	n/a
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?	n/a
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.	19
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	n/a

RFI Question		Paragraph #
	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?	n/a
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.	n/a
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?	1, 2
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?	1, 2, 3, 4, 14, 17, 19
4	What factors are important in determining whether bank-fintech arrangements support or hinder responsible innovation and a competitive and compliant financial services landscape?	1, 2, 3, 4