October 30th, 2024

Chief Counsel's Office
Attn: Comment Processing, Office of the Comptroller of the Currency
400 7th Street, SW
Suite 3E-218
Washington, DC 20219

Federal Reserve Board of Governors
Attn: Ann E. Misback, Secretary of the Board
Mailstop M-4775
2001 C Street, NW
Washington, DC 20551

James P. Sheesley, Assistant Executive Secretary
Federal Deposit Insurance Corporation
550 17th Street, NW
Washington, DC 20429

Re: Request for Information on Bank Fintech Arrangements Involving Banking Products and Services Distributed to Consumers and Businesses – Docket No. OCC-2024-0014, Docket No. OP-1836, RIN 3064-ZA43.

The Consumer Federation of America and Americans for Financial Reform Education Fund appreciate this opportunity to comment on improving the supervision of relationships between insured depositories and non-bank fintechs.

The Office of the Comptroller of the Currency, the Board of Governors of the Federal Reserve, and the Federal Deposit Insurance Corporation (the "Agencies") should increase their scrutiny of partnerships that involve banking as a service (BaaS) relationships. These arrangements should be considered high-risk and qualify for supervision under a stricter framework. Moreover, the Agencies should have supervision across the entire BaaS "supply chain."

A bank-fintech arrangement can break the interdependence that creates trust in banking. The financial stability of customers and the soundness of a financial institution should be linked. Banks can fail because the loans they have made go into default. When an unauthorized payment transfer made by a bank is compromised by fraud, such as with a check of a credit card purchase, the bank is held liable for most or all the losses. A consumer expects their bank to protect their funds and remedy the situation when there is

a problem. This structure leads to an alignment between the bank's financial goals and the consumer's financial health.

Due to the unique risks arising when the connection between a bank and its customers is severed, the Agencies must scrutinize these partnerships more. A bank charter is a privilege that provides financial and reputational benefits to its owners. As a result, those firms entrusted with a charter should be held to a higher standard. Consumers' expectations of a bank differ from those placed on a non-bank, but this distinction cannot be taken for granted. Given the dramatic increase in their number and the growing interest among consumers in using a product designed through BaaS, it is urgent to address this issue. From 2020 to 2023, the Agencies issued 23 enforcement actions against partner banks.[1] These actions will have a lasting impact on the sector. Nonetheless, loopholes remain. The next step is to gain supervisory authority over the non-banks, which play a vital role in partnerships.

I. Supervision of BaaS companies: The Agencies should insist that all banking-as-a-service firms are subject to supervision.

i. Non-banks that perform essential and foundational aspects of banking should be subject to consolidated supervision. The Banking Services Company Act provides a basis for their activities to fall under supervision.

ii. BaaS activities can be performed inside bank holding companies. Accordingly, the supervision of BaaS firms should not be viewed as a threat to innovation.

iii. Supervision is necessary because independent BaaS firms provide retail banking services but are not adequately accountable to consumers. Examinations of banks that partner with fintechs should be designated as "high-risk" and receive additional scrutiny.

II. Treatment of Fintech Deposits: The Agencies should apply greater scrutiny when assessing the safety of fintech deposits.

i. Deposit liabilities should be traceable to a specific depositor.

ii. Deposits sourced from fintech arrangements present risks and may counter reasonable and sustainable growth.

iii. Banks who rely on fintechs for most of their deposits may become overly dependent on those relationships. When a bank relies on a narrow set of relationships for its business (lending or deposit-taking, it raises concerns that the bank will be unduly influenced to take risks to meet the needs of its third-party partners.

iv. The 2020 brokered deposits rule should be revised. Fintechs that deliver deposits to insured depositories should be classified as deposit brokers, and the deposits in those arrangements should be defined as brokered.

v. Banks must have access to all consumer financial data to comply with the new Section 1033 rule.

III. Bank fintech arrangements must be accountable for complying with consumer protection laws.

i. *Partner banks must be held accountable for violations of community reinvestment expectations.*

ii. *People of color are more likely to be underbanked.*

iii. *BaaS products and nonbanks can create racialized impacts.*

[1] S&P Global. "Small Group of Banking-as-a-Service Banks Logs Big Number of Enforcement Actions," January 23, 2024. https://www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/small-group-of-banking-as-a-service-banks-logs-big-number-of-enforcement-actions-80067110.

IV. Arrangements that hold or manage non-fiat deposits or transfers.

i. Banking regulators should be able to supervise arrangements between banks and crypto fintechs that can pose unique risks to customers and depository institutions.

ii. Crypto-fintech-banking relationships pose unique risks for customers and for statutory compliance that warrants heightened regulatory scrutiny.

DISCUSSION

I. Supervision of BaaS companies: The Agencies should insist that all banking-as-a-service firms are subject to supervision.

iii. Non-banks that perform essential and foundational aspects of banking should be subject to consolidated supervision. The Banking Services Company Act provides a basis for their activities to fall under supervision.

The Banking Service Company Act (BSCA) requires depository institutions to notify their prudential regulator of contracts with service providers for certain activities. Covered activities include check and deposit sorting, posting and computation of interest, preparing and mailing statements, and other clerical or accounting functions. The BSCA subjects service providers to regulation and examination when performing functions that a depository institution would otherwise fulfill. The definition of a bank service company is broad but encompasses deposit services by companies that are themselves not deposit-takers. The BSCA explicitly applies to independent bank services companies owned partly by a depository and others that meet certain conditions.[2]

The BSCA gives prudential regulators the authority to examine some vendors to insured depositories if they perform "check and deposit sorting and posting, computation and posting of interest, preparation and mailing of checks or statements, and other clerical, bookkeeping, accounting, statistical, or similar functions such as data processing, online banking, and mobile banking services" and "such performance shall be subject to regulation and examination by the appropriate Federal banking agency to the same extent as if such services were being performed by the savings association on its own premises."[3]

This language certainly provides the foundation for Agencies to supervise all ledgering activities. Given the broad remit under online banking and mobile banking activities, there is a basis for the Agencies to supervise all the activities of BaaS companies completed on behalf of insured depositories.

Congress has given the Agencies the authority to assert supervisory power over independent BaaS companies.

iv. BaaS activities can be performed inside bank holding companies. Accordingly, the supervision of BaaS firms should not be viewed as a threat to innovation.

Many banks house a BaaS division within their holding company. Their existence underscores how BaaS can occur inside a supervised environment. BaaS firms can serve clients and exist inside the supervisory framework.

For example, when Fifth Third Bancorp purchased the BaaS provider Rize Money, Rize's activities were placed inside a supervised framework. Rize Money builds application programming interfaces (APIs) that

[2] 12 USC Ch. 18: Bank Service Companies.
[3] (D)7(d)i Deposits and Deposit Services. Regulatory Authority.

help banks process ACH, wire, and real-time payments.[4] Green Dot also has a large banking as a service division. Like all BaaS providers, Green Dot can match non-bank fintech clients with third-party vendors. For example, it has relationships with a tax software firm, a debit card printer, and an ATM network.[5] These are the essential benefits of BaaS. Fifth Third and Green Dot are only two of many examples. They underscore that supervision will not quash this industry.

iii. Supervision is necessary because independent BaaS firms provide retail banking services but are not adequately accountable to consumers. Examinations of banks that partner with fintechs should be designated as "high-risk" and receive additional scrutiny.

Intermediating the relationship between the consumer-facing brand and the insured depository breaks an essential safeguard in banking. Ideally, banks and their customers are aligned. When one prospers, so does the other. Their shared outcomes are further strengthened when the relationship between the bank and its customers is durable over time. Until the 1990s, there was no alternative version of this structure. All relationships between consumers and their banks were direct. Shadow banking and money market funds were the first examples of disintermediation.

Since the late 2000s, bank fintech arrangements have introduced new forms of disintermediation and created new supervision complexities. As of September 2022, a single regulator supervised ten institutions participating in over 50 product relationships.[6] New technologies and firm structures have entered the market, with the unfortunate result of blurring accountability. For example, FDIC insurance does not cover the failure of a fintech, even if the consumer perceives their primary relationship to be with the company whose name is emblazoned on their debit card.

Additionally, the fintech industry has introduced higher-risk forms of capital to retail banking. Whereas a chartered bank can access capital from the Federal Reserve at highly subsidized rates, fintechs draw their funds from private markets including venture capital and private equity. This is a very expensive and very short-term source of capital. As a result, most fintechs have to demonstrate their concept to their investors quickly. According to one large b2b fintech, startups have an average of 20 months to prove their model.[7] Most will not qualify for a new funding round without demonstrating their proof of concept. Inevitably, their constraints influence their decision-making and culture.

Fintechs will be drawn to the BaaS model because it offers an immediate and cost-efficient way to start a financial company. While it may cost tens of millions to be approved for a de novo bank charter, a startup can launch a new neobank debit card program with as little as $250,000 using a BaaS company.[8] The BaaS model also expedites the timeline.[9] Unfortunately, the BaaS model supports a system that fails regularly. Most fintechs do not succeed. Most fail – and in a few years or less. As a sector, the valuation of fintech companies has fallen dramatically since the beginning of the pandemic. Existing companies

---

4 Stutts, Jordan. "Fifth Third Targets Payments Expansion with Rize Money Acquisition." American Banker, May 22, 2023. https://www.americanbanker.com/news/fifth-third-targets-payments-expansion-with-rize-money-acquisition.

5 Green Dot Corporation. "Green Dot Debuts Embedded Finance Brand and Platform of Services, Arc by Green Dot," October 22, 2024. https://ir.greendot.com/news-releases/news-release-details/green-dot-debuts-embedded-finance-brand-and-platform-services/.

6 Hsu, Michael. "Safeguarding Trust in Banking: An Update." Remarks presented at the TCH + BPI Annual Conference, September 7, 2022. https://www.occ.gov/news-issuances/speeches/2022/pub-speech-2022-106.pdf.

7 Brex. "3 Ways to Extend Your Startup Runway and Reduce Cash Burn." Brex, September 7, 2024. https://www.brex.com/journal/startup-runway.

8 Wangoo, Radhika. "How Much Does It Cost to Build a Neobank App like SoFi?" Apptunix Blog, July 21, 2024. https://www.apptunix.com/blog/how-much-does-it-cost-to-build-a-neobank-app-like-sofi/.

9 Treasury Prime. *Accelerating Your Neobank Launch*. Ebook, 2023. https://go.treasuryprime.com/rs/253-WQB-828/images/AcceleratingYourNeobankLaunch_eBook.pdf?version=0.

that have customers but are not profitable will need additional rounds of funding, and if they do not receive it, they may also go out of business.

Risk-based supervision will help monitor activities by banks engaged in bank fintech arrangements. One solution is to provide more flexibility for regulators when reviewing banks that partner with fintechs. Regulators should be able to devote more resources and use more nuance when supervising "high-risk" arrangements. Bank fintech arrangements should be defined as high-risk.

Unfortunately, other players in the supply chain are not well-supervised. For example, many fintechs that process payments are regulated under state money transmitter licenses. This is a light form of supervision. It focuses on demonstrating compliance with specific procedures but avoids other areas of central importance – such as consumer redress in the event of failure. Others, such as database firms or cloud information technology providers, may not be supervised by any entity with any tangential relationship to financial services supervision. An independent BaaS middleware firm is probably curating services from lightly regulated fields, such as money transmission, with others outside the regulatory perimeter. However, their work is to provide a bank with a supply chain of banking services. Regulators must step in to address these new novel forms of banking. They must provide supervision across the supply chain.

II. The Agencies Should Apply Greater Scrutiny When Assessing the Safety of Fintech Deposits.

Deposits placed through third-party fintech relationships present unique risks. Regulators should strengthen rules defining when a deposit is brokered. Deposit liabilities should be traceable to specific depositors.

i. Deposit liabilities should be traceable to a specific depositor.

One of the practices that led to the problems with the Synapse failure was the use of "for benefit of" (FBO) accounts. While some bank partners avoid moving dollars into consortia because of the risks it entails,[10] others participate in these arrangements. Synapse moved deposits from Evolve Bank & Trust ("Evolve"), where they were initially placed, to FBO accounts at a consortium of other banks. The funds were held as liabilities to Synapse Brokerage when it made this shift. With these two steps, the attribution of each dollar deposit to a specific depositor was lost.

The decision to move funds from an account designated to a person and into one characterized as a liability to the fintech, as was the case with Synapse Brokerage, disadvantages the depositor. If a bank's records cannot identify the specific depositor of funds and the bank fails, the ability of deposit insurance to provide a remedy to depositors is lost. Importantly, consumers will not perceive the distinction when placing deposits with a fintech. Disclosures – even those sent to depositors in fall 2023 announcing the funds would be transferred into Synapse Brokerage – are fundamentally inadequate.

For these reasons, the guidance on third-party relationships should require that banks have a line of sight into ledgers. Evolve and fintech programs relied on Synapse to provide ledger reports. Ledgering is complex, with transfers settling at different times, with different durations between clearing and posting, with some vulnerable to reversal but others not, and through systems with varying degrees of reliability. It was the fault of Synapse for choosing a poor information technology system for its ledgering, but Evolve and depositors felt the impact of their decision. The problems that resulted when a non-bank was allowed to choose the provider for this critical banking activity underscore the difficulty when responsibilities for fundamental components of banking are divided among different vendors.

[10] Cross, Miriam. "What Is a BaaS Bank's Responsibility Post-Synapse Collapse?" *American Banker*, July 3, 2024. https://www.americanbanker.com/news/what-is-a-baas-banks-responsibility-post-synapse-collapse.

The Agencies must ensure supervised banks can see individual account balances in real-time, including cleared but not settled transactions, and receive a correct ledger at the close of every business day on the liabilities to each retail depositor. Ideally, redundancies would be embedded in the system, where the fintech and middleware firm reconciliations would flow in the correct cadence to the bank. This second aspect would help to prevent the disagreements between fintechs and banks that resulted in the Synapse crisis.

ii. Deposits sourced from fintech arrangements present risks and may counter reasonable and sustainable growth.

When partnerships lead to rapid deposit growth at a bank, its regulators should increase scrutiny of the institution to ensure that the changes do not create new risks. The FDIC recognizes that an institution's rapid increases in size – through internal growth or through acquisitions – can contribute to institutional stability risk, heighten the risk of failure, and impair the ability of the regulators to resolve the failed institution.[11]

Evolve grew too quickly – perhaps too quickly. Evolve's deposit base – the rate of increase in deposits held – has steadily grown. In June 2013, Evolve had $270 million in deposits. In November 2020, Evolve had $405 million in deposits. By June 2024, it held $1.1 billion.

As its deposits grew, the share sourced from fintech relationships increased. (See tables 1a, 1b, and 1c in the Appendices). The growth led to a higher share of demand deposits and, beginning in 2023, a sudden shift to using more brokered deposits. Meanwhile, the sum of time deposits – including CDs and money markets where an early withdrawal is discouraged – remained flat. Despite that, the share of loans with a duration of more than one year grew from 2018 to 2024.

Outputs from the Federal Financial Institutions Examination Council (FFIEC) call reports reveal Evolve's rapid growth. From 2015 to 2024, Evolve's deposit liabilities increased from $267 million to $1.1 billion. Its loan portfolio also grew from $299 million to $1.02 billion. During this time, the nature of Evolve's deposit liabilities shifted. In 2015, the share of Evolve's demand deposits held by individuals was 63 percent of the bank's deposits, but by 2024, the share was 100 percent. In 2015, time deposits made up 87 percent of all deposits, but by 2024, the share had fallen to 20 percent. Evolve ceased to have a diverse source of deposits, including corporations and partnerships. In summary, all of its deposits now come from households, and only a tiny fraction are time deposits.

In 2023, Evolve dramatically increased its use of brokered deposits. (Table 2) FDIC data shows that beginning in the second quarter of 2023, brokered deposits increased 178-fold, from 27/100ths of one percent of all deposits to 48.3 percent. Whereas it held on $4.1 million in brokered deposits in the first quarter of 2023, it had $612 million in the second quarter. At the end of June 2024, Evolve still had $441.5 million in brokered deposits.[12]

These trends reflect a deposit base with flight risk. Too often, the depositors of bank-fintech partnerships move funds in and out of their accounts quickly. Many online savings account depositors are yield chasers with no loyalty to the bank. The velocity of withdrawals made possible by digital banking

---

[11] *See* FDIC. Notice of Proposed Rulemaking for Resolution Plans Required for Insured Depository Institutions with More than $100 Billion or More in Total Assets. 88 Fed. Reg. 180. September 19, 2023 at 64579 et seq. https://www.govinfo.gov/content/pkg/FR-2023-09-19/pdf/2023-19266.pdf.

[12] BankRegData.com. "Evolve Bank & Trust Brokered Deposits." Accessed October 28, 2024. https://bankregdata.com/bkLQmet.asp?met=BRO&inst=HC1142411.

exposed how non-core deposits create run risks. In 2023, First Republic Bank had a run on uninsured deposits held in sweep accounts. Those deposits were not classified as brokered. If they had been, they would have triggered flags that are raised when a bank does not meet the standards for "well-capitalized." Among those responses would have been an action that prevented First Republic from renewing some of its contracts to hold brokered deposits.

Insisting on supervising a sponsor bank in the same manner as a traditional retail institution is a decision to prioritize consistency above common sense. Even if the bank is well-capitalized, the flight risk associated with fintech-sourced demand deposits and brokered deposits is greater.

Risk-based supervision will permit regulators to apply informed nuance. Sponsor banks often use their deposits for the same purposes as traditional ones – to lend "long." Supervision has developed to provide safeguards given this dynamic. However, bank fintech arrangements rely on a non-traditional and historically novel depositor constituency. As discussed above, there is little reason to believe a fintech-sourced customer whose funds are held at Evolve will remain so for three, ten, or fifteen years. This contrasts significantly with normal (non-fintech) primary account relationships, where consumers stay with their bank for 17 years, on average.[13] Under the current framework, Evolve can lend "long" like any other bank. Over half of Evolve's loan portfolio has a duration beyond three years, and approximately 40 percent is longer than five years.

Before 2020, banks with a high share of brokered deposits received additional scrutiny if they were not well-capitalized. The same skepticism should be applied when a bank has attracted a high share of its deposits through fintech relationships. One option would be to define any fintech deposit as brokered and then change the brokered deposit rule back to its approach before 2020.

> *iii. Banks who rely on fintechs for most of their deposits may become overly dependent on those relationships. When a bank relies on a narrow set of relationships for its business (lending or deposit-taking), it raises concerns that the bank will be unduly influenced to take risks to meet the needs of its third-party partners.*

Small banks with substantial bank partnership programs may face a conflict between safety and soundness expectations and deposit sustainability. This imbalance could compel a bank's management to circumvent essential procedures designed to protect the bank's capital base, prevent fraud and money laundering, and comply with consumer protection laws.

The decision-making by Evolve's management underscores how a bank could ignore clear signs of violations of the Bank Secrecy Act (BSA), anti-money laundering (AML), and know-your-customer (KYC) regulations. Evolve recognized that Synapse could not produce a reliable ledger as far back as 2018, and when the bank challenged Synapse on the issue, Synapse responded by blaming the bank.[14] The concerns involved questions about debits to FBO accounts and remote deposit capture of checks. The round of finger-pointing should have raised flags for regulators. Moreover, if Evolve felt it could no longer trust its BaaS partner, the bank should have terminated the relationship at that point. It did not.

---

13 Wisniewski, Mary. "Survey: Consumers Stick With Same Checking Account For 17 Years." Bankrate, January 4, 2022. https://www.bankrate.com/banking/how-long-people-keep-their-checking-savings-accounts/.

14 Mikula, Jason. "$13M in Missing User Funds: Evolve, Synapse Play Blame Game as BaaS Crisis Intensifies." Substack newsletter. Fintech Business Weekly (blog), October 8, 2023. https://fintechbusinessweekly.substack.com/p/13m-in-missing-user-funds-evolve.

New discrepancies continued to emerge. In September 2022, Synapse alerted Evolve that it had not received timely ACH return files, resulting in 41,500 late transactions and lost funds owed to Synapse.[15] In November 2022, Evolve's controller sent a letter to Synapse complaining that its understanding of balances held in FBO accounts differed from Synapse's by a staggering sum of a "couple hundred million on the daily." In July 2023, Synapse asked Evolve's accounting firm to audit data for one week. In doing so, it discovered discrepancies of $6.5 million due to gaps and duplications of ACH and remote deposit capture transactions. It is not clear if a request was made to audit another week.

Notably, Evolve never abandoned the relationship. Why? Most likely, the reason was related to the fact that between 60 and 70 percent of Evolve's deposits were attributable to a single fintech – Mercury. This fintech used Synapse. Evolve could have ended the relationship with Synapse but would have lost this fintech's business. Leaving Synapse would have, in effect, required the bank to sell most of its loan portfolio to meet requests for its demand deposits.

The counterfactual argument – that Evolve did not need Mercury and would have stayed with Synapse irrespective of the presence of Mercury – was disproven in September 2024. On September 25th, Evolve secured an agreement with Mercury to cease to intermediate with Synapse. Instead, Mercury would work with Evolve directly. On September 27th, having secured Mercury's business, Evolve terminated its contract with Synapse.

When a bank sources the preponderance of its deposits from only one or a handful of third-party relationships, it creates risk. The Agencies must identify an undue concentration of deposits from only a few fintech partners as a high-risk activity. Risk concentrations may occur frequently due to the prevalence of partner banks under $10 billion in assets. While some industry voices may contend it would undermine the sector's viability, it does not matter.

Moreover, the problem is pressing. Some very large deposit-facilitating fintechs partner with small banks. It is not unreasonable to believe they can assert a high level of influence on the decision-making of their small bank partners. For example, the largest debit card fintech uses two partner banks. One has $4 billion in assets, of which $3.7 billion consists of demand deposit liabilities,[16] and the other has $8.1 billion in assets, including $7.1 billion in deposit liabilities.[17] Reports suggest the fintech has 7 million active accounts.[18] The fintech opens 20,000 new accounts every day. Were the fintech to leave either bank – but particularly the smaller one that does not have many other fintech partners – it would create a deposit outflow that could cripple the institution. The prudential regulators should clarify in the guidance that concentrations of deposits based on a single relationship with a BaaS partner or a single fintech are high risk.

iv. The 2020 brokered deposits rule should be revised. Fintechs that deliver deposits to insured depositories should be classified as deposit brokers, and the deposits in those arrangements should be defined as brokered.

Agencies have distinguished between deposits received from consumers (individuals, businesses, and organizations) and those sourced through marketplace arrangements. The latter has been judged to pose more uncertainty.

---

15 ibid

16 Federal Financial Institutions Examination Council. June 30, 2024. Call report for Stride Bank, NA.

17 Federal Financial Institutions Examination Council. June 30, 2024. Call report for Bancorp Bank, NA.

18 Kauflin, Jeff. "Exclusive: The Inside Story of Chime, America's Biggest Digital Bank." Forbes, May 3, 2024. https://www.forbes.com/sites/jeffkauflin/2024/05/03/exclusive-the-inside-story-of-chime-americas-biggest-digital-bank/

The 2020 rule created a new framework for defining a brokered deposit. It exempted arrangements where deposits are at a single depository from restrictions placed on brokered deposits. It increased the number of exceptions for business relationships excluded from the deposit broker designation. The rule was deregulatory in nature. Unfortunately, it reduced barriers to risk and may have shrouded risk-taking from regulatory oversight.

The single depository exception created loopholes that led to consumer harm. Several fintech companies had bank partnerships to accept deposits to facilitate the trading of digital assets. When valuations of crypto assets fell in 2022, several large fintech companies failed. Consumers with accounts at crypto company Voyager, who exchanged their fiat deposits for non-fiat stablecoin, suffered losses. While common sense would have identified this structure as high-risk, Voyager was not considered a deposit broker solely because all the funds Voyager received from customers were placed at a single bank.[19]

Banks that derive deposits from fintechs rely on brokered deposits. At the end of q2 2024, almost 40 percent of Evolve's deposits were brokered. (See Table 2 in the Appendices.) Evolve's reliance was not unique. Other banks working with Synapse had similar profiles. For example, 63.1 percent of Lineage Bank's deposits were classified as brokered at the beginning of 2024, and 13.6 of American Bank (Le Mars, Iowa) were similarly defined.

Moreover, the rule change may have obscured risks at partner banks that did not use Synapse. For example, Bancorp Bank (Sioux Falls, South Dakota) is a bank partner to many fintechs. From 2014 to the first quarter of 2020, between 75 and 88 percent of its deposits were categorized as brokered. After the rule change, the share fell immediately to 30 percent and is now at 6 percent.[20] Pathward Bank, formerly known as MetaBank, has a similar pattern. While its share of brokered deposits was near 60 percent for the prior six years, the reported number dropped to 7 percent in q2 2021 and is now at 1.6 percent.[21] The practices at these institutions have not changed.

v. Banks must have access to all consumer financial data to comply with the new Section 1033 rule.

The Section 1033 rule states that consumers own their financial data and that banks must make it available to them in a timely, machine-readable format upon request. Additionally, the rule establishes expectations for consumers to control how their data is used, shared, and retained.

Unless a financial institution has direct access to ledgering information, it cannot comply with this rule. Consumers must have the protections afforded to them by Section 1033. Accordingly, the Agencies must ensure that BaaS companies give banks access to the data.

III. Bank fintech arrangements must be accountable for complying with consumer protection laws.

In BaaS arrangements, the different components of a fintech product are fulfilled through intermediaries. The only centralizing force behind the product is the middleware BaaS company itself. Because of the chimeric aspect of the arrangements, essential elements of trust and experience may be short-circuited, and accountability may not be clearly assigned. Compliance may be viewed pejoratively as a cost center in this setting, and providers may compete on least-cost conditions.

---

[19] Sanneh, Ebrima Santos. "FDIC Reverses Course on Trump-Era Brokered Deposits and ILC Rules." *American Banker*, July 30, 2024. https://www.americanbanker.com/news/fdic-reverses-course-on-trump-era-brokered-deposits-and-ilc-rules.
[20] BankRegData.com. "Bancorp Bank Brokered Deposits." Accessed October 28, 2024. https://bankregdata.com/bkLQmet.asp?met=BRO&inst=HC2858951.
[21] BankRegData.com. "Pathward Bank Brokered Deposits." Accessed October 28, 2024. https://bankregdata.com/bkLQmet.asp?met=BRO&inst=HC2390013.

The Agencies must ensure that bank fintech arrangements do not amplify existing inequalities in our banking system. Adequate supervision must protect Black, Latine, and other financially vulnerable populations.

i. Partner banks must be held accountable for violations of community reinvestment expectations.

Bank partnership models allow a bank to grow, even if it has community reinvestment shortcomings that would prevent a bank from growing through traditional methods like opening new branches or acquiring another bank. In 2013 and 2017, Evolve received a substantial noncompliance CRA rating. This rare outcome put the bank among only a fraction of a percent of financial institutions to receive such a low rating. The rating would have prevented Evolve from acquiring new banks or opening new bank branches, but it would not have prevented it from attracting deposits through partnerships with fintechs.

In its 2013 performance evaluation, the Federal Reserve noted that Evolve had been the subject of enforcement actions for violating the terms of the Equal Credit Opportunity Act (ECOA), the Fair Housing Act (FHA), and Section 5 of the Federal Trade Commission Act in 2013. In the 2017 CRA performance evaluation, one reason for the substantial noncompliance rating was for evidence of substantive violations of the ECOA and the FHA.

Regulators should prohibit any partner bank from contracting to establish new BaaS-enabled fintech relationships if the financial institution has a less-than-satisfactory CRA rating. The difference in methods should not be the basis for a distinction in regulatory treatment.

ii. People of color are more likely to be underbanked.

Systemic racism has created an environment that has left people of color, particularly Black and Latine customers, as well as people with limited English proficiency (LEP), more likely to be underbanked due to lower credit scores.

Credit scores are critical to determining who is approved for credit and at what prices and terms by mainstream financial firms (banks, insurance, credit cards, vehicle dealers, etc.). However, credit scoring often replicates the financial system's systemic racial biases because Black and Latine consumers with lower incomes, more medical debt, lower homeownership rates, fewer assets, and less credit history are deemed less creditworthy by the credit reporting companies.[22] Black and Latine consumers who have credit scores tend to have lower average credit scores than white consumers (8 percent and 5 percent lower, respectively).[23]

But these averages obscure far higher levels of subprime scores or no credit scores for Black and Latine consumers. The Consumer Financial Protection Bureau found that Black and Latine consumers were about 60 percent more likely to have no or invisible credit scores than white consumers (28 percent, 27 percent, and 16 percent, respectively).[24] A 2022 Urban Institute study found that there were far more people with subprime credit scores in Black, Indigenous, and Latine communities than in white communities (41 percent, 43 percent, 29 percent, and 17 percent, respectively).[25] These stark credit score

[22] National Consumer Law Center. "Past Imperfect: How Credit Scores and Other Analytics 'Bake In' and Perpetuate Past Discrimination." May 3, 2016.
[23] Sandberg, Erica. "How race affects your credit score." *US News and World Report*. August 9, 2022.
[24] Brevoort, Kenneth P., Philipp Grimm, and Michelle Kambara. Consumer Financial Protection Bureau. "Data Point: Credit Invisibles." May 2015.
[25] Urban Institute. "Credit Health During the COVID-19 Pandemic." March 8, 2022.

disparities present a significant barrier to financial inclusion and traditional banking services because they are a determining factor in accessing credit, insurance, housing, employment, and more.

iii. BaaS products and nonbanks can create racialized impacts.

BaaS products must be regulated to protect underserved households and communities, strengthen their economic security and resilience, promote broad-based economic growth, and reduce economic inequality for these populations. Consumers – particularly lower-income Black, Latine, and Indigenous consumers who often lack access to generational wealth, comprehensive fiduciary investment advice, or sustainable credit – can ill afford exposure to this type of risk, harm, and volatility.

The fintech companies providing app-based, platform-based financial services (for payments, credit, or savings) are increasingly providing some financial services to geographies and demographics underserved by mainstream financial providers. But these fintech services offer complex terms, hidden fees, insecure privacy and limited data protection, few consumer protections, and, ultimately, costly products. These fintech products are poorly regulated and often skirt federal banking regulatory oversight to offer quasi-bank products through affiliations with banks chartered in states with weaker consumer protections and higher usury caps (a process known as rent-a-bank).[26]

Cryptocurrencies and other digital assets and platforms represent the most recent and visible example of these fintech patterns. Many crypto products and services constitute a form of predatory financial inclusion, with promoters pushing crypto products as supplanting traditional banks and the need for essential governance, sound regulation, and oversight. Though the crypto industry claims that the underlying technology can make all financial services cheaper, faster, and more secure, the industry's documented track record shows a very different trajectory.

Responsible supervision and stronger protections must be established for an equitable, safe, and sound marketplace that protects Black, Latine, and other people of color. Financially vulnerable populations are more likely to be underbanked, less financially well-off, and less able to access traditional banking services – conditions substantially rooted in a historical and ongoing legacy of structural racism in housing, employment, healthcare, and education. It is essential to prevent further negative impacts and risks of these products from perpetuating these racial inequities going forward.

IV. Arrangements that hold or manage non-fiat deposits or transfers.

i. Banking regulators should be able to supervise arrangements between banks and crypto fintechs that can pose unique risks to customers and depository institutions.

The Synapse case has also shone a light on bank-fintech-crypto arrangements that introduce an additional layer of complexity, uncertainty, and risk for customers. A key client of Synapse and Evolve was Juno Finance. Juno advertises itself as an "on-ramp" to twenty or more blockchain crypto platforms for its users, and it offers services meant to streamline the transfer of fiat currencies held in bank accounts to crypto platforms.[27] In particular, Juno promotes on its

[26] CFPB. CFPB v. Think Finance, LLC. Complaint. U.S. District Court of Montana, Great Falls Division. November 15, 2017 at 25.
[27] Juno Finance Homepage. Access October 29, 2024. https://juno.finance/

website the platform's ability to speed up certain types of transfers between banks and crypto platforms.[28]

It has done this in part by offering access to basic banking services – checking accounts and hi-yield savings accounts via its partnership with Evolve and Synapse. Additionally, Juno created facilities for its customers to invest in crypto, including receiving rewards in crypto, access to crypto trading platforms, access to crypto wallet providers, and the option to convert portions of customer's paychecks into crypto once received.

Juno's easy conversion of currency into cryptocurrency was a magnet for scammers that was impossible for Synapse and Evolve to police. Sources inside Synapse described Juno as "nightmare fuel" for Synapse and Evolve's compliance team. These sources described Juno as a "preferred haven for Nigerian scammers," who used the accounts to carry out scams that "varied but spanned the entire scammer world" – "[d]rop accounts (money mules), business email compromise scams, tax scams, romance scams (often the money mules), payroll intercept scams, Zelle, all of it."[29]

Juno's business model should have raised red flags. Records of Juno accounts made public as a part of Evolve's recent hacking breach demonstrated clear compliance risks: many accounts sharing the same address, including Juno's officer headquarters; phone numbers with country codes from India (despite the account's U.S. postal address); missing identity information for account holders; and more. Reportedly, the financial crime issues with Juno were so severe and persistent that "for an extended period, Synapse held weekly tri-party meetings with Evolve and the company to attempt to address the situation, according to the former Synapse employee."[30]

The Juno example underscores how gaps in regulatory compliance by banks and their fintech partners can be exacerbated when fintech clients such as Juno offer products and services associated with high-risk activities, geographies, or entities in crypto ecosystems.

Figure 1 is a spreadsheet revealing the business locations of cards sent by Juno and the location of the devices from which applicants applied for accounts. In these examples, the devices were located in foreign countries. Some were in countries on OFAC lists. Many of the business locations were identical. Such overlaps seem improbable, primarily because they were located in small rural towns that were unlikely to have large office buildings at the same physical address. Despite these glaring concerns, the accounts were issued. Indeed, the fact that no party had put in place simple algorithms to spot foreign device locations or repeated addresses is so contradictory to common sense that it should have led regulators to conclude that Evolve had permissive KYC standards in place intentionally. The bank may have built a business model around non-compliance with essential laws.

---

[28] Juno Finance Blog. "Why is Coinbase Holding My Funds?" March 15, 2024. https://juno.finance/blog/why-is-coinbase-holding-my-funds

[29] Mikula, Jason. "Synapse Program Was "Nightmare Fuel" Due to Control Gaps, Ex-Employee Says." Fintech Business Weekly, July 21, 2024. https://fintechbusinessweekly.substack.com/p/synapse-program-was-nightmare-fuel?utm_source=publication-search

[30] *Ibid.*

Figure 1: Mercury accounts flagged by Evolve connected to Juno

Phone First 3	Country Code	Address Type	Permission	City	Country	ZIP	Street	State	Deposit US Bal
923	Pakistan	PO Box	LOCKED	CLOVIS	US	93611	1187 N WILLOW AVE # 103-812	CA	0.67
923	Pakistan	PO Box	LOCKED	CLOVIS	US	93611	1187 N WILLOW AVE # 103-839	CA	82.03
923	Pakistan	Reg Agent	CLOSED	SHERIDAN	US	82801	1309 COFFEEN AVE	WY	116.17
923	Pakistan	Reg Agent	CLOSED	SHERIDAN	US	82801	1309 COFFEEN AVE STE 1200	WY	210.28
923	Pakistan	Reg Agent	CLOSED	SHERIDAN	US	82801	1309 COFFEEN AVE STE 1200	WY	110.08
923	Pakistan	Reg Agent	SEND AND RECEIVE	SHERIDAN	US	82801	1309 COFFEEN AVE STE 1200	WY	1307.8
923	Pakistan	Reg Agent	SEND AND RECEIVE	SHERIDAN	US	82801	1309 COFFEEN AVE STE 1200	WY	1072
971	UAE	Reg Agent	SEND AND RECEIVE	SHERIDAN	US	82801	1309 COFFEEN AVE STE 1200	WY	488.38
798	Russia	Reg Agent	CLOSED	SHERIDAN	US	82801	1309 COFFEEN AVE STE 1200	WY	9.59
923	Pakistan	Reg Agent	CLOSED	LEWES	US	19958	16192 COASTAL HWY	DE	0.5
923	Pakistan	Reg Agent	CLOSED	LEWES	US	19958	16192 COASTAL HWY	DE	0.68
923	Pakistan	Reg Agent	CLOSED	LEWES	US	19958	16192 COASTAL HWY	DE	0.44
923	Pakistan	Reg Agent	CLOSED	LEWES	US	19958	16192 COASTAL HWY	DE	675.62
923	Pakistan	Reg Agent	LOCKED	LEWES	US	19958	16192 COASTAL HWY	DE	2175.8
923	Pakistan	Reg Agent	LOCKED	LEWES	US	19958	16192 COASTAL HWY	DE	55.03
790	Russia	Reg Agent	CLOSED	LEWES	US	19958	16192 COASTAL HWY	DE	4.51
791	Russia	Reg Agent	SEND AND RECEIVE	LEWES	US	19958	16192 COASTAL HWY # 14/3	DE	856.25
971	UAE	Reg Agent	SEND AND RECEIVE	SHERIDAN	US	82801	30 N GOULD ST	WY	4094.71
923	Pakistan	Reg Agent	CLOSED	SHERIDAN	US	82801	30 N GOULD ST STE 22596	WY	0.01
923	Pakistan	Reg Agent	CLOSED	SHERIDAN	US	82801	30 N GOULD ST STE 23609	WY	1227.26
923	Pakistan	Reg Agent	CLOSED	SHERIDAN	US	82801	30 N GOULD ST STE 23983	WY	1
971	UAE	Reg Agent	SEND AND RECEIVE	SHERIDAN	US	82801	30 N GOULD ST STE 24157	WY	0.84
923	Pakistan	Reg Agent	CLOSED	SHERIDAN	US	82801	30 N GOULD ST STE 24446	WY	0.14
923	Pakistan	Reg Agent	CLOSED	SHERIDAN	US	82801	30 N GOULD ST STE 24614	WY	0.02
923	Pakistan	Reg Agent	SEND AND RECEIVE	SHERIDAN	US	82801	30 N GOULD ST STE 24632	WY	0.12
923	Pakistan	Reg Agent	CLOSED	SHERIDAN	US	82801	30 N GOULD ST STE 25211	WY	2.64
923	Pakistan	Reg Agent	CLOSED	SHERIDAN	US	82801	30 N GOULD ST STE 4000	WY	0.12
923	Pakistan	Reg Agent	LOCKED	SHERIDAN	US	82801	30 N GOULD ST STE 5042	WY	3.12
923	Pakistan	Reg Agent	CLOSED	SHERIDAN	US	82801	30 N GOULD ST STE 7134	WY	0.91
923	Pakistan	Reg Agent	CLOSED	SHERIDAN	US	82801	30 N GOULD ST STE R	WY	3.07
923	Pakistan	Reg Agent	CLOSED	SHERIDAN	US	82801	30 N GOULD ST STE R	WY	0.09
923	Pakistan	Reg Agent	SEND AND RECEIVE	SHERIDAN	US	82801	30 N GOULD ST STE R	WY	475.6
971	UAE	Reg Agent	CLOSED	SHERIDAN	US	82801	30 N GOULD ST STE R	WY	0.07
971	UAE	Reg Agent	CLOSED	SHERIDAN	US	82801	30 N GOULD ST STE R	WY	28.6

source: Fintech Business Weekly[31]

Regulators should recognize that crypto-fintech-banking business arrangements are high-risk and should exercise heightened oversight over how AML and sanctions compliance responsibilities are shared and distributed amongst parties in these banking-fintech arrangements. This should include directing the parties to detail how these responsibilities and legal liabilities are delineated in their contracts or services agreements.

ii. Crypto-fintech-banking relationships pose unique risks for customers and for statutory compliance that warrant heightened regulatory scrutiny.

Crypto-based or crypto-enabled fintechs can pose risks to customers when even one link in the bank-fintech supply chain falters. When Synapse collapsed in May 2024, Evolve took over processing ACH transactions on behalf of Synapse's Brokerage account holders, including for Juno and its customers. Soon after, Evolve halted card payments for Juno customers and stopped processing incoming ACHs and wires. Evolve took such action because they lacked access to a key software function previously provided by Synapse, according to court proceedings.[32]

[31] Mikula, Jason. "Evolve Hack Crisis: Russia-Linked Cybergang Leaks Records On Millions." Substack newsletter. *Fintech Business Weekly* (blog), June 30, 2024. https://fintechbusinessweekly.substack.com/p/evolve-hack-crisis-russia-linked.

[32] Juno Finance Blog. "Latest updates on banking and card services." May 20, 2024. https://juno.finance/blog/latest-updates-on-banking-and-card-services

As a result, Juno customers had their accounts frozen and were unable to use or transfer those funds. This had serious impacts on customers who were not only using their Juno accounts for crypto-related transactions but also functionally as banking or payment vehicles. News reports have profiled consumers who assumed that because Juno named Evolve as its FDIC-insured banking partner, their accounts were safe—only to have tens of thousands of dollars frozen in their Juno accounts for weeks.[33]

As discussed above, the misleading advertising associated with bank-fintech relationships regarding FDIC coverage as well as the mismanagement of ledgers and custody of customer deposits require rigorous regulatory supervision and examination. This example shows how such problems can touch even customers who believe they are using a product like crypto that purportedly sit outside traditional banking services.

An increasing number of bank-fintech-crypto partnerships raise similar and additional questions. Many of these "banking as a service" offerings rely on webs of interconnected providers to deliver the service, including chartered banks. The complexity of the fintech and crypto supply chain leaves customers vulnerable to weak consumer protections or unfair terms buried in multiple user agreements, potential fees or charges imposed by any of the service providers, and frailties if any provider in the supply chain cannot perform their role. One example is the Coinbase Card. Coinbase's debit card allows its holders to make point-of-sale (POS) purchases using crypto they hold in a Coinbase wallet. The card is promoted as a seamless way to use crypto as a means of payment, precisely as a customer would use a debit card issued by a bank to depositors. Yet, the process that is needed to facilitate crypto point-of-sale payments is far more complex than using a bank's debit card. The Coinbase Card relies on at least four service providers to perform the advertised function of using crypto to make retail purchases.

First, customers need to open two accounts. They must have a Coinbase wallet to be eligible for the Coinbase card. The Coinbase wallet receives crypto rewards from using the card and is the source of the funds for transactions. And since Coinbase is not a chartered bank, it partners with Pathward (a South Dakota bank) to issue a debit card. In effect, to initiate the use of this card, users authorize Coinbase to create a new deposit account with Pathward, which receives and is the custodian of the funds deposited into an account that is linked to the customer's Coinbase wallet. The Pathward Coinbase Card is not a transaction account card (like a debit card associated with a checking account), it is a pre-paid, stored-value card. Coinbase's terms of service warns customers to treat the card the same as cash, not as a savings or checking account.[34]

Coinbase Card customers load the card from their Coinbase wallet and convert the crypto into U.S. dollars. Coinbase card users can also set up direct deposit of funds from an employer or payroll provider into their pre-paid account.[35] Customers can spend down the dollars they pre-

---

[33] Son, Hugh. "How thousands of Americans got caught in fintech's false promise and lost access to bank accounts." CNBC, July 3, 2024. https://www.cnbc.com/2024/07/02/synapse-fintech-fdic-false-promise.html

[34] Coinbase Cardholder Agreement. Accessed October 14, 2024. https://assets.ctfassets.net/q5ulk4bp65r7/sEhBc9st9Ws5He4te6bYi/85a632727687193a6ffc871b99e9642b/Coinbase_CHA_October_14_2024.pdf

[35] "User Agreement - Coinbase." Accessed October 31, 2024. https://www.coinbase.com/legal/user_agreement/united_states.

loaded onto the card or authorize the transfer of crypto to the pre-paid card at the point of sale, but that adds conversion fees for converting into USD at the transaction time.

Second, the payment processing relies on a third-party provider to complete the transaction. The Coinbase card uses the Visa payment network as payment rails, which provides nearly universal merchant acceptance. The user agreements for the cards (from Pathward and Coinbase) stipulate that Pathward is responsible for the payment aspects of this transaction, including payment dispute resolution. Coinbase mostly facilitates the sale of crypto for customers, including for immediate use as a means of payment.

Finally, a fourth provider converts crypto into U.S. dollars, which is necessary to make a retail point-of-service transaction. Coinbase relies on the fintech platform Marqueta to help facilitate the instantaneous sale of the customer's crypto assets. Marqueta does this in several ways. First, when customers use a card at a point-of-sale location, Marqueta issues a "Just-in-Time" funding call to Coinbase – essentially a request by the client to sell assets from their Coinbase wallet. Marqueta also provides user interface tools that allow Coinbase to show cardholders the crypto transaction confirmation, the price received in dollars for selling the crypto used in the POS purchase, and other functions. In a role characteristic of BaaS providers, Marqueta also says it facilitates communications with cardholders regarding aspects of card issuance, such as card creation details and cardholder statements (even though the card itself is issued by Pathward).

Marqueta also states that Coinbase relies on its service to help handle Know your Customer (KYC) obligations and card fulfillment.[36] Financial institutions and many fintechs are required to understand the identity, suitability, and risks posed by their customers as part of their compliance with anti-money laundering and illicit finance laws and regulations. Marqueta's contention that it handles KYC obligations either conflicts with or overlaps with Pathward's role as stated in the Coinbase Cardholder Agreement, which lays out Pathward's KYC obligations as well as the requirements its cardholders must meet to be able to receive a card from Pathward.[37] Neither the Coinbase user agreement nor Marqueta's promotional materials clarify what exactly Marqueta does concerning KYC.

The complexity of these banking-fintech arrangements can make it harder to enforce consumer protections, anti-money laundering, or other financial regulations and leave customers vulnerable to fees and fine-print consumer protection limitations in multiple agreements. There may be nothing untoward about the Coinbase Card arrangements; in some cases, they clearly delineate the responsibility and roles of the named parties in this arrangement. However, it illustrates the complexity of these arrangements and raises questions about what happens to customers when things don't work according to plan. Moreover, it highlights the importance of regulatory oversight and supervision to protect customers and enforce statutory obligations. For example:

---

[36] Marqeta. "Coinbase Case Study: Leading Cryptocurrency Platform Uses Modern Card Issuing to Unlock New Financial Opportunities for Customers," https://www.marqeta.com/asset/coinbase?x=hj28Ub. https://www.marqeta.com/asset/coinbase?x=hj28Ub.

[37] Coinbase, and Pathward Bank, NA. "Coinbase Card Cardholder Agreement," 2024. https://assets.ctfassets.net/q5ulk4bp65r7/sEhBc9st9Ws5He4te6bYi/85a632727687193a6ffc871b99e9642b/Coinbase_CHA_October_14_2024.pdf.

- *Potential gaps in anti-money laundering and know-your-customer compliance:* Coinbase ostensibly conducts KYC when users first create accounts (and wallets). When Pathward conducts KYC on potential new Coinbase card holders, does it conduct the same level of review? Is its review more extensive? Does it rely on information Coinbase provides on its users or conduct its own review? If Marqueta says it is involved in facilitating KYC for Coinbase for the issuance of the Coinbase card, exactly what role does it play in that process (an important question given what we know about gaps in AML compliance with respect to Evolve and Synapse)?

- *Customers with disputes must navigate multiple parties' dispute processes:* Because each transaction relies on the actions of multiple entities, it can be difficult for customers to reach a satisfactory resolution for potential transaction errors. Pathward appears to lay out its statutory obligations for payment and dispute resolution in its terms of service, but what happens if an error occurs because of actions Marqueta took or failed to take? For example, if Marqueta makes an error in reporting the current market value of a crypto asset being used for payment, a customer would have their funds converted at less than market value. The Coinbase user agreement states that it is not responsible for errors with respect to these crypto sales that facilitate payment activities. Is it responsible for errors associated with the sale and conversion of crypto assets in this instance, even if the error stemmed from Marqueta's actions?

- *Selling assets to finance point-of-sale transactions can create tax liabilities for users:* Although Coinbase states that the Coinbase Card stored value card should be used and considered cash, if customers sell crypto assets to fund POS purchases, they could expose themselves to taxable liabilities. Coinbase states that, in some cases, the sale of a client's crypto assets may constitute a taxable event if the assets sold have appreciated in value and represent taxable capital gains. Is Coinbase responsible for providing their client with tax reporting information for these asset sales, or are they treated differently because of their use for point-of-sale purchases? Recent IRS rulemakings would suggest that Coinbase is responsible.

- *Customers could face forced crypto transactions to finance POS purchases:* Both Coinbase and Pathward note that if a user has insufficient funds to cover a purchase, both platforms reserve the right to initiate the sale of crypto assets held in the associated Coinbase wallet sufficient to cover the expense. What happens if such a sale has a knock-on effect on the Coinbase wallet user with respect to their investment or trading activity – say, if it affects their ability to cover their other obligations or trading strategies for another crypto asset, derivative, or future? Can customers forgo the POS purchase to avoid crypto asset sales, and are they informed of pending or potential transactions from their wallet that might create financial costs for the user?

- *So-called Just-in-Time crypto transactions can have lag times that create financial costs for users:* Coinbase and its partner Marqueta give the impression that the sale and conversion of crypto assets for payment use with this card can and do happen quickly. However, crypto transactions can be delayed either for technical reasons or to allow time for any party (the bank, the fintech, or the crypto provider) to review the transaction. Customers could be

exposed to potential losses if the price of the crypto assets being sold to finance the POS purchase declines between when the transaction is initiated by the user and when the transaction is completed by Marqueta or Coinbase. The volatility of crypto prices could expose users to significant asset price declines. The purchaser might not have used those assets for the purchase had they known the processing time would affect their value. Are card users simply left to bear that risk, or are there circumstances in which the other parties are liable? How does the cardholder know their obligations and the issuers' obligations and/or exercise their rights?

- *Personal and financial information can be exposed by many more parties in these complex transactions:* Who is responsible for data privacy and cybersecurity standards throughout this transaction chain?

The complexity of the Coinbase Card fintech supply chain demonstrates the need for increased regulatory oversight of these banking-fintech relationships that can expose customers to risks and impede compliance with banking laws. These and other fintech-crypto product offerings where crypto assets and crypto intermediaries are more directly involved in payment activity in concert with banking institutions are becoming more commonplace. There needs to be more oversight and clarity regarding all parties' rights, responsibilities, and obligations. The Coinbase Card likely represents the more conventional end of the bank-fintech-crypto relationship spectrum. Other reported types of crypto debit card partnerships seem less clear and potentially even more concerning, including promoting "no-KYC" cards or cards linked to self-hosted DeFi wallets.

Regulators should recognize that crypto-facing bank-fintech arrangements like the Synapse-Juno and Coinbase Card create heightened risk for customers and the financial system. The crypto business model itself—without adding a banking-fintech-crypto relationship—poses many risk factors to counterparties, consumers, and the broader financial system. Regulators should consider bank-fintech arrangements with a crypto component constituting greater risk and impose more proactive supervision and oversight by banking regulators.

Conclusion

Thank you for the opportunity to comment on these critical questions. The Agencies must act swiftly to address the uncertainties created by bank fintech partnerships that use independent non-bank banking-as-a-service firms. A loophole has permitted unsupervised institutions to perform essential banking functions for too long. The recent crisis demonstrates the need for a response. We call on the Agencies to use their authority under the Banking Service Company Act to assert supervisory authority over companies when they conduct banking activities on behalf of chartered financial institutions. Please reach out to our organizations if we can provide further clarifications.

Sincerely,

Consumer Federation of America
Americans for Financial Reform Education Fund

Appendices

Table 1a: Evolve's loan portfolio, 2015 to 2024 (Schedule RC-C)				
Loans	30-Jun-15	30-Jun-18	30-Jun-21	30-Jun-24
< 3 months	$40	$149	$179	$276
3 to 12 months	$21	$31	$78	$38
1 to 3 years	$19	$66	$85	$113
3 to 5 years	$52	$123	$111	$188
5 to 15 years	$26	$19	$40	$49
More than 15 years	$141	$22	$34	$358
Total	$299	$410	$527	$1,022

Table 1B: Evolve's deposit composition, 2015 to 2024 (Schedule RC-E)				
	30-June-15	30-June-18	30-June-21	30-June-24
Individuals + Corporations + Partnerships + Demand Deposits	$34	$144	$362	$918
Demand Deposits (share of A)	$21	$122	$330	$918
Time Deposits + money markets	$233	$226	$146	$225
	$267	$370	$508	$1,143

Table 1c: Metrics of deposits and loans				
	30-Jun-15	30-Jun-18	30-Jun-21	30-Jun-24
loan to deposit ratio	1.12	1.11	1.04	0.89
Time Deposits/ All deposits	87%	61%	29%	20%
Loans > 1 year/all loans	79.5%	56.1%	51.2%	69.2%

Table 2: Share of deposits from brokered relationships, Evolve Bank & Trust, 2015 to 2024	
Year.quarter	Percentage
2015.2	0.4
2016.2	0.4
2017.2	10.4
2018.2	10.1
2019.2	6.7
2020.2	4.7
2021.2	2.7
2022.2	2.1
2023.2	48.3
2024.2	38.6

Source: FFIEC via BankRegData