

TRUSTLY, INC., MATTHEW JANIGA

Proposal and Comment Information

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

Comment ID: FR-0000-0134-01-C131

Submitter Information

Organization Name: Trustly, Inc.

Organization Type: Company

Name: Matthew Janiga

Submitted Date: 10/30/2024



Trustly, Inc.
555 El Camino Real
San Carlos, CA 94070

October 30, 2024

Chief Counsel's Office
Attention: 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 St. NW, Washington, DC 20551

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

Submitted via Regulations.gov portal

Re: Request for Information on Bank-Fintech Arrangements Involving Banking Products and Services Distributed to Consumers and Businesses—RIN 3064-ZA43

Dear agency staff:

I'm writing on behalf of Trustly, Inc. ("Trustly") a global leader in open banking payments. Trustly appreciates the opportunity to comment on the request for information about bank and non-bank arrangements. While our full comments are below, we wish to highlight the following:

- We are appreciative of the efforts that prudential regulators have made to understand non-bank business models and the opportunities and risks we may present to the banking industry. Key staff at the OCC, Federal Reserve and FDIC have helped foster a great dialogue with the fintech industry over the last decade, both in Washington and in key fintech cities like San Francisco. We are excited to see these dialogues continue into the next Presidential administration.
- The RFI presents a good overview of current bank-fintech arrangements, their risks and opportunities, but we would encourage staff to further segment payments arrangements into card/ACH/wallet merchant payment acceptance and card/wallet issuance offerings.
 - The non-bank merchant payment acceptance market is substantially more mature than the fintech card/wallet issuance market. This means that non-bank merchant acceptance companies benefit from a broader and more experienced talent pool and a deeper total addressable market. Both of these hallmarks of a mature market lead to decreased risks to banks that partner with merchant acceptance fintechs.

- Non-bank merchant acceptance is a B2B product, with few, if any, direct consumer touch points. This contrasts with issuance and wallet products, which are sold directly to consumers and governed by consumer regulations like Regulation Z and Regulation E.
- We would encourage staff to further segment merchant acceptance into enterprise, SMB and developer segments. Enterprise merchant acceptance processors present fewer risks to the banks that serve as partners, as they have smaller, well-known and well-resourced customer bases when compared to SMB or developer offerings. In contrast, SMB and developer focused merchant processors may have to keep track of millions of private company customers and sole proprietors when those processors reach scale. This can introduce complexity and risk into KYC, sanctions and transaction monitoring functions. Developers, who often sell intangible software products, also present different AML and terrorist financing risks than SMBs who sell physical goods and may maintain physical store fronts.
- Open banking data access arrangements are not formal partnerships, nor should they be. Companies like Trustly do not provide services to the bank under these arrangements, and no fees or revenue are exchanged. Some large banks have taken very adversarial approaches to open banking data sharing, which serves to frustrate a consumer's intent to share data. We hope these banks cease these adversarial actions now that the CFPB has finalized its Section 1033 rule.

I. About Trustly and our U.S. Operations

Trustly is a global leader in open-banking powered payments and now regularly processes more than \$100 billion annually in merchant payments across our European and North American markets. Trustly, on behalf of its merchants, is also one of the largest RTP originators and accounts for approximately ten percent of all RTP volume on a quarterly basis.¹ Trustly's U.S. business offerings have helped modernize ACH payments and offer faster payments to consumers and merchants across a variety of operational and compliance tasks. Trustly primarily helps its merchant partners through three product lines.

- **Trustly Connect** — an account and routing number validation service, confirming consumer ACH payment account numbers via open banking data and commercially available third-party account validation services.
- **Trustly ID** — a service to support a merchant's account creation and risk management functions. Trustly ID allows a consumer to share his or her bank account data so that a merchant may receive the consumer's full name, mailing address, email address and telephone number listed on the bank account.
- **Trustly Pay** — Trustly's flagship offering. Trustly Pay allows merchants to ask Trustly to use open-banking data to evaluate the fraud and risk of payment transactions, then process the transactions for merchant acceptance purposes. Trustly offers merchants (i) a simple, verified ACH account processing option, (ii) a partial guarantee for settlement risks (NSF, administrative returns) or (iii) a full guarantee (NSF, administrative, stopped, unauthorized & frozen returns).

Trustly predominantly works with large, enterprise-scale merchants that have well-established data protection and customer support functions. Trustly performs underwriting and diligence on all merchants prior to them being able to access the Trustly services. Our merchants range across a variety of

¹ See <https://us.trustly.com/press/trustly-cross-river-lead-rtp-adoption>.

industries and include all of the major U.S. communications providers, FAANG companies, leading online marketplaces, leading remittance providers and online sports betting operators.

Trustly acts as a joint user of open banking data. Merchants will hire Trustly to perform various payments related tasks using the data, while consumers provide their affirmative consent for Trustly to access and use the data. This includes Trustly asking the consumer to agree to terms of use and acknowledge Trustly's privacy policy. When using the consumer's data, Trustly complies with the numerous overlapping state and federal laws related to data privacy and data security. Because of the size and prominence of our merchants, we adhere to several extra-judicial data protection and privacy requirements that are required by our merchants' commercial agreements. This use of open banking data will also soon be subject to Section 1033.

We are committed to ensuring consumers have a superior experience when using our product. Trustly maintains a 24x7x365 consumer-facing customer service function that includes email, chat and phone support via a "request a call" option. We are exploring the use of chat bots and AI agents, but will always make it easy for customers to reach a human support team member.

II. Regulatory Requirements and Oversight of Trustly's Business

Some in the policy arena are prone to use the talking point that non-banks are not regulated and do not play by the same rules as banks. Trustly disagrees with this categorization, as consumer protection and privacy laws are triggered by the products a company offers and apply equally whether the offering is coming from a bank or non-bank. Trustly, and several of our peer companies in the open banking and merchant acceptance spaces, are also supervised under a variety of state and federal regimes.

Where Trustly acts as a payment processor, our business largely falls under the agent-of-payee exemptions in federal and state law. This means these business activities are not subject to explicit regulatory requirements. We are still subject to UDAP and UDAAP laws, sanctions laws, privacy laws and industry requirements such as those found in the NACHA rules and operating guidelines. Our bank ODFI partners also impose various AML, diligence and audit requirements via contract.

Trustly has been obtaining money transmission licenses for future product activities, including some background operational changes for our payouts product. The first of these products will be a B2B offering so that corporate customers may use Trustly's open banking and payouts capabilities to send payments to their customers. Trustly relies on the RTP, FedNow and ACH systems to send these payments. All payments are domestic to the U.S., and no senders or funds move across borders.

Pursuant to our money transmission licenses, Trustly is subject to state-led regulatory exams. Many states have modernized their money transmission laws to have more stringent capital and balance sheet requirements, driven largely by the adoption of a tangible net worth concept and corresponding thresholds. State-led exams often focus on AML, sanctions, consumer complaints and consumer protection laws. As detailed below, some states are starting to focus on data security. Larger money transmitters will trigger FinCEN examinations, generally conducted by IRS examiners under an MOU to provide supervision staff. Money transmitters are also expected to file SARs and must produce several monthly, quarterly and annual reports on transaction volume and financial performance to state regulators. This includes reporting audited financial statements and disclosing beneficial owners — especially foreign owners.

Trustly's use of open banking data has generally been subject to UDAP, UDAAP and state and federal privacy laws. With the CFPB's publication of its Section 1033 rule, Trustly's use of open banking data will soon be subject to the new Section 1033 requirements for data aggregators and authorized third

parties. Trustly's current operations are already materially aligned with the CFPB's final section 1033 rule, and we do not expect to need to make material changes to our operations or product in response to the rule. While we do not expect any material adjustments to our business, ticking and tying the last mile of compliance with the rule will still require a company-wide effort and take us several months.

We understand the CFPB has been conducting supervisory examinations of open banking data aggregators. While Trustly is primarily an authorized third-party data recipient with how it uses open banking data in its payment acceptance products, we expect the CFPB will conduct a supervisory examination of our U.S. business and its use of open banking data in the near future.

We do not offer consumer-facing payments products at this time, so we do not expect to be subject to the CFPB's larger participant payment supervision process. We may offer consumer-facing products in the future, which would likely trigger supervision under the rule.

III. Data Security Practices in Trustly's Business

Many policy makers and consumer advocates are concerned that open banking induces consumers to share their online banking login credentials with a variety of third parties. The recently finalized Section 1033 rule is meant to address this policy matter by shifting the U.S. open banking market to API access that will eliminate credential sharing. But this transition will take time, given the lengthy compliance periods provided to data providers under the final 1033 rule.

Because we and our merchants share policy makers' concerns, Trustly has developed a patented, split token method to safeguard consumer online banking credentials. For years, Trustly has used this split token method to safely secure consumer credentials. The process works as follows:

- Consumers choose to use Trustly's services with their merchant, triggering our user interface. During this process, consumers receive disclosures making them aware that Trustly will access their banking data and share it with the merchant.
- After agreeing to Trustly's terms and privacy policy, the consumer will enter their online banking credentials.
- Trustly will place the consumer's credentials into its token encryption process. This technology puts the consumer's login credentials into an encrypted token.
- Trustly then splits this encrypted token into two parts on a randomized bit-by-bit basis, sending half to the consumer's merchant and retaining half on Trustly's systems.
- Trustly only recalls the merchant's half of the token when the merchant requests Trustly to perform an open banking job that requires access to the consumer's current banking data. This is almost always done because the consumer is requesting a service such as choosing to pay the merchant via an ACH debit. During these open banking jobs, Trustly will rejoin the two parts of the token and decrypt the credentials so Trustly can login to the consumer's bank account on that consumer's behalf. Trustly then separates the tokens and eliminates the merchant's half from Trustly's systems.

This split token process means that there is only ever a split second where Trustly is in possession of the consumer's full online banking credentials. This effectively reduces the risk of a data breach involving the consumer's credentials to zero, as there is no database of consumer credentials on Trustly's system to be exfiltrated in a breach scenario.

It is also worth noting that Trustly — like many of our late stage and publicly-traded peer non-bank technology companies — uses large technology data security and control practices. We encrypt data in transit and at rest. We use least-privilege access, where internal staff have access to the minimum amount of data necessary to do their jobs. We have a documented data security program, regularly engage in penetration and other security testing, require employee data security training and undergo annual SOC 1 and SOC 2 audits.

Trustly, like some non-bank payments companies, also holds several state money transmission licenses. While these state regulators have often focused on AML, sanctions, financial safety and soundness and consumer protection issues, more and more of them are conducting a review of data security programs. And New York state has a formal data security regulation and data breach reporting requirement for licensees, something the state reviews during onsite examinations.

IV. Types of Bank Arrangements in Trustly's Business

Trustly's business model currently involves the following bank arrangements:

A. Data access arrangements — Trustly needs to access a consumer's data that is held by the consumer's bank to offer our products. Consumers direct Trustly to access this bank-held data and share it with Trustly's merchants for payments and onboarding use cases. These arrangements are not partnerships and Trustly is not providing services to the bank. Sometimes banks even take an adversarial approach to Trustly's business, something we hope ends with the promulgation of the Section 1033 rule.

There are three general types of data access arrangements —

- **Formal Data Access Agreements** — some banks, particularly large banks that have open banking APIs, will offer Trustly the ability to enter into a contract with the bank. This contract allows Trustly the ability to access consumer data via the bank's open banking API, in exchange for certain commercial commitments from Trustly. Many of these commercial commitments are typical, common sense provisions that impose industry-standard data security requirements and requirements that Trustly will comply with applicable law. But sometimes these agreements function as contracts of adhesion, with the bank using their market dominance to impose onerous terms that can work to frustrate consumer access to data and consumer access to new products and services.

These agreements — and the underlying APIs — vary in slightly different ways. This means that sometimes Trustly can launch a product using one bank's data, but may not be permitted to offer consumers at another bank the same product. This also means that banks introduce unnecessary complexity into the U.S. open banking market. This complexity is ultimately helpful for Trustly as it creates an unintentional moat for our business, but we would prefer a more uniform and efficient market.

- **White Listing Agreements** — Many banks have yet to develop an API to offer open banking data. Some of these banks will enter into agreements to whitelist Trustly's data access traffic. This is beneficial to the bank, because they do not need to worry that the incoming traffic is malicious and therefore they can focus IT security resource on other potential intrusive data traffic. Trustly in turn benefits from banks not blocking our legacy connection methods.
- **No Agreement** — Many banks do not have the capacity to enter into a formal agreement with Trustly, and some larger banks remain outright hostile to open banking data sharing. In these

instances, Trustly uses its legacy connection methods to access consumer bank data at the direction of the consumer. Trustly does not use headless browsing or screen scraping. Additionally, Trustly only pulls data from the bank's systems when it is needed to process a consumer request. These two points often mean that Trustly is not a strain on the bank's IT systems, and many times Trustly's data sharing process is not even noticeable to the bank.

B. ODFI Agreements — Trustly maintains several agreements with banks for ODFI and related non-card payment services. These contracts allow Trustly to offer ACH debit, ACH credit, RTP and FedNow services to merchants. To access these services, Trustly will either access a bank-provided API or assemble a file of transactions in the relevant format for the other payment systems. RTP transactions also need to be pre-funded during normal banking hours. Trustly will arrange for its merchants to relay wires or fund ACH debits to the banks that support Trustly's RTP activities. The bank will then rely on its own IT provider, often one of the large core providers, to submit the transactional information to the relevant payment network.

These ODFI agreements also generally involve the use of FBO accounts. Some of these accounts are held in the name and taxpayer identification number of Trustly's bank partner. Others are held in Trustly's name and taxpayer identification number. Trustly assists with the reconciliation of the accounts. Because these accounts are held for dozens of enterprise-level merchants, reconciliation of these accounts does not present the same complexity or risk as reconciling an FBO with funds owed to thousands or millions of consumer customers.

C. Open Banking Services Agreements — In some cases, Trustly is providing open banking data and related services to a bank. Some banks have agreements with Trustly to access open banking data for account opening purposes. Other banks partner with us to offer our guaranteed ACH product to their customers, but with the bank retaining the activities associated with ACH payment functions.

D. General Corporate Treasury Services — Trustly also maintains corporate banking relationships for treasury services, such as holding Trustly's corporate funds.

V. Feedback on Selected Questions from the RFI

We hope the above information helps your organizations better understand current merchant acceptance practices, especially those that involve open banking data. We believe the above information will also be responsive to several questions from the RFI.

Below, please find responses to selected additional questions from the RFI.

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?

The RFI appears to combine card issuance activities and structures along with wallets and general merchant acceptance activities. We would recommend that the OCC view merchant acceptance — both of card payments and ACH transactions — as a separate category from wallets and card issuance activity. This is because the operations of merchant acceptance companies are often simpler, and involve significantly less risk of loss or consumer harm than wallet and card issuance businesses.

Enterprise merchant acceptance companies — who work with a smaller number of large, public and well-known businesses — also present less AML and sanctions risks than those processors that work with SMBs. This is due to the notoriety and scale of enterprise merchants — having McDonalds or Walmart as a customer does not present the same KYC questions as serving a few million sole proprietors. Enterprise-focused processors also tend to have a few hundred or thousand well known, large customers. In contrast, products that serve smaller private companies, sole proprietors and software developers can have millions of lesser-known, harder to identify customers to KYC and monitor.

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?

We believe that banks benefit from partnering with non-bank payment acceptance companies. We provide banks a new source of fee income with a manageable set of compliance and operational risks. The fact that Trustly is regulated at the state level and regularly undertakes financial, control and data security audits, also helps minimize the operational and compliance risks we might present to partners.

Banks who partner with Trustly to obtain our open banking data services also benefit by being able to access new technologies that they otherwise may not have the scale or expertise to build themselves.

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?

As the OCC is aware, ODFIs will receive NACHA files that list all transactions to be run through the bank. Trustly transmits similar RTP and FedNow data to its bank partners for our payouts offering. Trustly also transmits KYC and KYB files about its enterprise merchants, including non-AML related diligence on a merchant's financial standing and business operations. This allows Trustly's ODFI partners to ask questions and approve of new merchants before their transactions start running through the bank.

Because the bank receives all transactional data as well as all KYC and KYB onboarding data, we do not believe there is any difference from the information a bank would receive if it offered the ACH payment service directly to merchants and without Trustly.

In the merchant acceptance space, an ODFI will almost always require Trustly to perform transaction monitoring. Because the transaction is running through the bank, Trustly will file unusual activity reports to the bank, which allows the ODFI to file a SAR as necessary under the institution's policies and procedures. However, none of this prevents the bank from using the transaction data sent via the NACHA or other payment file to conduct its own AML transaction monitoring and SAR investigation program.

Trustly will also generally provide audited financial statements, our independent AML assessment and other audit reports, which allow the bank to monitor other elements of our business and ask for additional information if the audits present a concern or risk.

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?

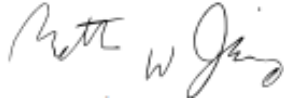
Trustly and the bank generally do not involve other key service providers in the product's operations, nor do they place intermediaries between Trustly and the bank. Trustly may assemble and process merchant payment transaction data, and the bank uses its existing IT infrastructure to submit those data files to the relevant payment system.

Trustly and the bank may have their own key service providers to operate each side of our respective businesses. For example, Trustly hosts its software on one of the leading cloud providers. We would consider this cloud service provider to be a material vendor to Trustly. We believe that the banking regulators, via FSOC, have been reviewing cloud service providers to determine if any of them might present systemic risks to the U.S. financial systems. Our use of a leading cloud service provider to host all of our operations and software functions would present another potential risk touchpoint for the banking industry. We believe several other merchant acceptance companies also use cloud providers to host their software, which may further compound any actual or potential risks to partner banks.

* * * *

Thank you for the opportunity to respond to the RFI. Should you have any questions or wish to discuss our comments, please feel free to contact me and Matthew Faso, Senior Banking Partnerships Manager.

Regards,



Matthew Janiga
Director, Regulatory and Public Affairs
Trustly, Inc.