Trustly, Inc.
[redacted]

September 18, 2025

Via Electronic Submission to Regulations.gov

Office of the Comptroller of the Currency 400 7th Street SW Suite 3E-218 Washington, DC 20219

Board of Governors of the Federal Reserve System Ann Misback, Secretary 20th Street and Constitution Avenue NW Washington, DC 20551

Federal Deposit Insurance Corporation Jennifer M. Jones, Deputy Executive Secretary 550 17th Street NW Washington, DC 20429

Re: Request for Information on Potential Actions To Address Payments Fraud [Docket ID OCC-2025-0009; Docket No. OP-1866; RIN 3064-ZA49]'

Dear Comptroller, Board and Corporation Staff,

Trustly, Inc. ("Trustly") appreciates the opportunity to provide comments in response to the Request for Information (RFI) on potential actions to address payments fraud, issued by the Office of the Comptroller of the Currency (OCC), the Board of Governors of the Federal Reserve System (Board), and the Federal Deposit Insurance Corporation (FDIC).

Trustly has extensive experience helping merchants and consumers shift from check and card payments to modern, non-card payments such as ACH, Real Time Payments ("RTP"), and FedNow. We process over $100 billion annually in non-card payments across North America and Europe and are one of the largest RTP originators, handling more than $10 billion in RTP payments each year.

This letter starts by providing an overview of how non-card payment methods have dealt with fraud and validation issues in the past. It continues with an overview of how Open Banking is helping Trustly and its Fortune 500 customers prevent non-card payment fraud and risk. We conclude by offering comments on specific questions from the RFI.

I. Open Banking's Importance to Reducing Payment Fraud

One cannot assess the current U.S. payments landscape without highlighting the importance of open banking, especially in modernizing non-card payments such as ACH. Prior

to open banking, accepting ACH required a business or government entity to validate the payor's ACH number. Doing this was a cumbersome process and often riddled with errors, fraud and operational risks.

One method was for the business or government entity to check the payor's ACH number against a commercial database. However, this method creates several issues for the payor and payee. First, the payor must accurately type in their ACH number because fat finger errors will cause the number to fail the database look up. Next, the payee must connect to multiple third-party commercial databases to find the payor's ACH number. This is because no third-party commercial database contains 100% coverage of American ACH numbers. Another risk comes from the fact that these third-party databases often contain outdated information. This means an account may be marked as valid when it is actually closed, and in some cases consumers may be flagged as having negative payment data when they are good payors. This locks consumers out of the ability to pay by check or ACH. If these same consumers are not able to access payment cards due to credit scores or negative data in third-party banking databases like Early Warning, then these consumers are effectively locked out of digital payments.

Another legacy method to validate ACH payment numbers was to run micro deposits. This is often found in a business context, where a company can onboard a business to an accounts payable/accounts receivable system and validate the bank account by sending a few cents worth of funds. The account holder then confirms the amount has been received into their bank account, and the account is thereafter deemed valid.

Open banking has materially simplified the account validation process, and in turn has also materially improved data quality and reduced fraud. Rather than do database lookups or slow micro deposits, payees can now ask a payor to log into their online banking and use that process to share an ACH number. Under NACHA rules, this number is deemed valid and the payee may start running payments against the number and associated bank account.

These benefits are more than theoretical. By way of example, all three of AT&T, T-Mobile and Verizon use Trustly to obtain and validate payor ACH numbers, and have been doing so for years. These companies have used our technology to shift their subscribers from paying via card to paying instead via ACH, saving hundreds of millions in card-based interchange as a result. By using ACH, these companies are also able to avoid legacy check lockbox processing operations and fees.

II. Responses to Specific RFI Questions

Responses to General Questions (Questions 23-26)

23. What types of payments fraud have most impacted your organization and its stakeholders? What tactics have criminals employed when perpetrating these types of payments fraud?

The most significant and costly type of fraud impacting our organization is first-party fraud facilitated by the weaponization of so-called "tokenized" account numbers or “TANs” injected into open banking data sets by certain large card-issuing banks. While these numbers are purported to offer consumer benefits, they have become a primary tool for fraudsters.

The tactic is straightforward: a fraudster uses the tokenized number to authorize an ACH debit for goods or services. The banks that issue these numbers then provide clear instructions to the consumer—in this case, the fraudster—on how to stop the payment from being funded by simply revoking open banking data sharing access. The result is that the fraudster receives the goods or services, but the ACH debit is never successfully completed.

This specific fraud vector regularly costs Trustly eight figures in annual fraud losses. Merchants who use our guaranteed ACH offering are largely protected from these losses. But merchants who use other providers have sometimes chosen to turn off pay-by-bank for the banks that inject TANs into open banking. This prevents consumers from these banks from being able to access the lowest cost payment method, which in turn sometimes means they cannot access the pricing benefits or rewards tied to pay-by-bank transactions.

24. What measures, including technological solutions or services, have been most effective in identifying, preventing, and mitigating payments fraud at your institution?

The most effective technological solution for modernizing payments and reducing operational risks associated with ACH payments has been open banking. Prior to open banking, validating a consumer's bank account for an ACH payment was a cumbersome process reliant on database lookups or slow micro-deposits, both of which were prone to errors, outdated information, and consumer friction.

Open banking has materially simplified this process by allowing a payee to ask a payor to securely log into their online banking to share a validated ACH number. This has dramatically improved data quality and has enabled major billers like AT&T, T-Mobile, and Verizon to shift millions of subscribers from card and check payments to ACH, saving hundreds of millions of dollars in interchange and processing fees. However, the effectiveness of this solution is being actively undermined by the fraudulent use of tokenized numbers, as described above.

Open Banking’s benefits extend beyond validating ACH account and routing numbers. Open Banking transactions almost always allow a business to check the name, address and contact information listed on the bank account. This allows businesses to have access to high-fidelity data that *should* match the keyed in information presented by the consumer.

When these records do not match in material ways, it is often a sign that the business may be dealing with a fraudulent customer or payment and therefore should apply more scrutiny to the transaction.

Similarly, Open Banking transactions can provide the types of payment security benefits seen in Europe under their Strong Customer Authentication ("SCA") standards. In Europe, SCA requires online payments to authenticate the payor via two of three authentication standards: (1) something the payor knows, (2) something the payor has and (3) something the payor is, such as a biometric or fingerprint. U.S. Open Banking payments can easily provide two of these SCA-like protections. First, payors must "know" their online banking credentials to set up Open Banking payments. Further, Trustly's testing has found that more than 75% of consumers using our services have elected to use their bank's multi-factor authentication processes. This means consumers must be in possession of something only they control — a phone or email account — to receive and use the multi-factor authentication code.

It is also noteworthy that these security measures exceed those found on a traditional payment card transaction, as hackers with access to a cardholder's PAN, expiry and CVV can fully pretend to be the cardholder. Whereas a hacker with someone's online banking credentials will not be able to easily or scalably have access to the consumer's phone or email account, preventing them from signing up for most pay-by-bank services.

In addition to the largely ubiquitous security features baked into the U.S. Open Banking landscape, Open Banking payments companies have built in their own additional fraud and risk prevention systems. For example, Trustly will check payors against our internal database of the 50+ million American payors that have previously used our products. We have the ability to identify repeat good and bad actors, and can deploy additional models and rules to identify fraudsters who are using new devices or credentials. Like many others, we also layer in protections from fraud consortium data that helps us digital fingerprint data such as device IDs that have previously been used in fraud schemes.

Responses to Regulation and Supervision (Questions 9-15)

9. What potential changes to regulations... could address payments fraud and mitigate the harms from payments fraud to consumers, businesses, and supervised institutions?

We believe anti-competitive and fraudulent behaviors by large banks are encouraging payment fraud against merchants, crypto exchanges and non-bank payments companies. We believe regulators could take several actions to combat these actions by the largest banks, including:

- **Prohibit Anti-Competitive Debanking:** Large card-issuing banks have refused to grant non-bank payment companies like Trustly essential ODFI relationships, often citing shifting and pretextual regulatory concerns under direction from their payment card divisions. Regulators should prohibit banks from using faux regulatory or reputational risk to deny banking services to lawful competitors in the payments space.

- **Regulate and Restrict the Use of Tokenized Account Numbers:** The "tokenized" account numbers that have been weaponized for fraud must be reformed. We recommend that regulators require banks to offer consumers a clear choice on whether to use a tokenized number and to provide clear disclosures that using such a number may prevent them from accessing certain payment types, such as FedNow.

- **Enforce the Durbin Amendment:** Large issuers are now attempting to charge fees for open banking data access, particularly for payments use cases. While these fees are currently being negotiated between market participants (often under duress), it is possible that some proposed fees would exceed the Durbin Amendment's cap on debit fee revenue for large banks. We request that the Board investigate whether these proposed fee structures violate the Durbin Amendment's pricing caps. At the very least, the Board should consider updating its FAQs so large issuing banks do not use open banking fees to circumvent the Durbin pricing limits.

- **Make Antitrust Referrals:** It appears that large issuers may be colluding to erect fee barriers, prevent competitors from accessing bank-controlled fraud and risk databases such as EWS, and generally take actions to slow the adoption of fraud-reducing non-card payment methods. Where warranted, we believe that the federal banking agencies should refer potential violations of law to the antitrust division of the Department of Justice, as these actions likely violate competition and price fixing laws due to the banks' abuse of their dominant market positions. We believe the banks have taken these courses of action against crypto companies, in addition to non-bank payments companies like Trustly.

- **Preserve the Section 1033 Open Banking Rule:** The CFPB's final rule under Section 1033 creates a regulated framework for open banking that is essential for modernizing payments. Any effort to vacate this rule would eliminate the legal right for consumers to share their financial data and would create material headwinds for the transition to modern, less-fraudulent electronic payments. The federal banking agencies should work with the CFPB to keep the final rule in place.

- **Address Fintech Barriers:** Fintech program managers like Chime have been hostile to non-card payment use cases, specifically blocking open banking payment companies from connecting to their accounts. This locks their customers out of modern payment options that may help reduce fraud. The Section 1033 rule would address this by requiring such companies to allow authorized third-party access. We have also seen

some fintech programs be a hotbed for fraudulent activity, which may signal that their partner banks are not providing sufficient oversight on suspicious activity and Red Flags issues.

Consumer, Business, and Industry Education (Questions 5-8)

7. Which approaches could make existing payments fraud education more effective?

One of the most effective approaches would be to prevent supervised institutions from actively misleading consumers. One of the largest credit card issuers sends emails to consumers claiming that open banking and ACH payments are unsafe, using this as a pretext to steer the consumer toward using one of the bank's own high-cost credit cards. Preventing this type of "scaremongering" would be a more effective educational tool than traditional regulatory efforts like informational fact sheets, as it would stop the spread of harmful misinformation at its source.

Reserve Banks' Operator Tools and Services (Questions 21-22)

22. Are there risk management tools or services that the Reserve Banks should consider offering or expanding...?

A critical issue is that large credit card issuers are ensuring the tokenized account numbers they inject into open banking data sets are incompatible with the FedNow Service. These numbers are designed to work only with The Clearing House's RTP system, an entity owned and controlled by those same large banks. This tactic currently locks approximately 30% of U.S. consumers out of using FedNow for open banking payments, a figure we expect to grow to over 50%. The Federal Reserve, in its operator role for FedNow, should investigate this practice and consider implementing rules or standards that ensure account numbers provided via open banking are interoperable with all payment rails, including FedNow.

We have also seen repeated barriers and walled gardens when it comes to fraud and risk data. While some fraud and risk data is freely available to any company, the fraud and risk data in the bank-controlled EWS offering has been made off limits for fintechs and payments companies. We believe the actions of certain large banks to block our access to EWS data are anticompetitive and merit investigation by banking regulators as potential debanking. We also believe this conduct should be referred to the Department of Justice's antitrust division for further review, especially since it runs counter to the types of commitments the bank-controlled The Clearing House Payments Company made to DOJ when it asked for pre-clearance of the RTP system.[1]

[1] DOJ response to TCH, Dated September 21, 2017, accessible at https://www.justice.gov/atr/page/file/998201/dl?inline=

Should America's largest banks persist in their anti-competitve business practices, including de-banking and no-banking crypto and payments companies, it may make sense for the Federal Reserve to create its own fraud and risk database. We offer no view on whether this would require a new statutory authority. However, there are parallels to how the Federal Reserve operates its own version of ACH and faster payments rails via FedNow to compete with the ACH and RTP offerings of the bank-controlled The Clearing House.

* * * *

Thank you for the opportunity to provide comments on this critical RFI. Modernizing the U.S. payments system and combating fraud requires an open and competitive ecosystem. We urge the agencies to address the anti-competitive barriers erected by incumbent institutions that not only stifle innovation but actively facilitate payments fraud.

Should you wish to discuss further, feel free to contact me at [redacted]

Regards,
Matt Janiga
Director, Regulatory Affairs
Trustly, Inc.