September 18, 2025

Chief Counsel's Office
Attn: comment processing
Office of the Comptroller of the Currency
400 7th St. SW, Suite 3E-218
Washington, DC 20219

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

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

RE: Request for Information on Potential Actions to Address Payments Fraud; OCC Docket ID OCC-2025-0009, Federal Reserve Docket No. OP-1866, FDIC RIN 3064-ZA49

Dear Secretary Misback, Deputy Executive Secretary Jones, and Chief Counsel:

Thank you for the opportunity to provide comments on fraud prevention.

The Consumer Federation of America (CFA) is an association of nearly 200 non-profit consumer organizations that was established in 1968 to advance the consumer interest through research, advocacy, and education. CFA works to advance pro-consumer policies on a variety of issues before Congress, the White House, federal and state regulatory agencies, state legislatures, and the courts. We communicate

and work with public officials to promote beneficial policies, oppose harmful ones, and ensure a balanced debate on issues important to consumers.

Last year, consumers reported losing more than $12 billion to fraud.[1] As markets and technology evolve, fraudsters have demonstrated their ability to pivot and exploit vulnerabilities in our financial infrastructure. As daunting as the Federal Trade Commission's (FTC's) numbers are, the problem is probably far worse. Reports of fraud inevitably undercount the true extent of the damage since most fraud is never reported. In 2021, a former FTC economist estimated that only 4.8% of victims reported their losses to the government or the Better Business Bureau.[2] Regulators must find new solutions to solve the skyrocketing rates of fraud occurring in our banking system.

Prudential regulators have significant authority to level the playing field between victims and criminals. If permitted to persist, fraud will undermine trust in banking, diminish the public's understanding of the difference between non-bank fintechs and insured depositories, and impose billions in costs.

Questions 1 to 8: External Collaboration; consumer business, and industry education.

Question 2. What types of collaboration, including standard setting, could be most effective in addressing payment fraud? What are some of the biggest obstacles to these types of collaboration?

Standards-setting organizations (SSOs) can apply outcome-based rules to hold institutions accountable for permitting fraud. NACHA has standards that deny merchants access to ACH services if the percentage of transfers that received complaints exceeds certain thresholds.[3] Over time, many of the high-risk activities identified by these rules took place when banks served businesses in high-risk business sectors: online gambling, adult entertainment, and other industries. They can also establish rules for the performance of critical fraud prevention technology.

To be effective, SSOs must apply meaningful penalties for non-compliance with their rules to participating financial institutions. To do that, SSOs must have some level of enforcement authority over their members. While it cannot be a substitute, rules established by SSOs can complement the enforcement work of regulators.

Question 5: In general, what types of payment fraud education are most effective, and why? Would different audiences (for example, industry and consumers) benefit from different types of payment fraud education?

- **AND -**

---

[1] Federal Trade Commission. (2025). *Consumer Sentinel Network Data Book 2024*. https://www.ftc.gov/system/files/ftc_gov/pdf/csn-annual-data-book-2024.pdf

[2] Anderson, K. B. (2021). *To Whom Do Victims of Mass-Market Consumer Fraud Complain?* (SSRN Scholarly Paper No. 3852323). https://doi.org/10.2139/ssrn.3852323

[3] NACHA. (2015, September 18). *ACH Network Risk and Enforcement Topics*. https://www.nacha.org/rules/ach-network-risk-and-enforcement-topics

Question 6: Would additional education informing consumers and businesses about safe payment practices can be helpful to reduce payment fraud and promote access to safe, secure payment options?

Consumer education is essential, but it cannot be the primary mode of defense against fraud. Consumer education campaigns consisting only of warnings for the "buyer to beware" will not be effective.

With advancements in generative artificial intelligence, the efficacy of scammers will only grow. More people will be challenged to correctly distinguish between a request from a friend and a scammer. Consumer education can be helpful, but by itself, it will be inadequate. However, regulators can encourage banks to take concrete steps to improve how they inform account holders about risks.

App providers should educate account holders on fraud from inside the app interfaces.
Increasingly, consumers are required to assess which text messages and social media inquiries are entreaties from criminals. The telecommunication companies and social media platforms do not effectively police their domains, and given that they earn revenue from criminals, the latter are motivated to preserve the status quo. One bank reported that half of the fraud reports it receives come from social media platforms.[4]

Given the success of criminals in devising convincing schemes, payment app providers should integrate warnings into the payment order process. Regular messages describing new types of scams, if conveyed inside their services, could potentially thwart some scams.

Make the use of multifactor authentication mandatory.
Education that consists of warnings only shifts responsibility from financial institutions to consumers, but without any meaningful help. To be more effective, education should provide consumers with advice on tools they can use to improve their account hygiene. Such an approach is akin to the use of safety belts: admonitions by manufacturers to drivers to be more careful are far less helpful than installing safety belts and instructing drivers on their value.

The use of multifactor authentication is one example. For example, the use by depositories of multifactor authentication (MFA) is currently considered a best practice for internet banking.[5] Some banks still do not use MFA. The prudential regulators should clarify their guidance on this subject to state that MFA is a required practice.

Reduce fragmentation in consumer fraud reporting.

---

[4] Au-Yeung, J. H. and A. (2025, May 15). Meta Battles an 'Epidemic of Scams' as Criminals Flood Instagram and Facebook. *Wall Street Journal*. https://www.wsj.com/tech/meta-fraud-facebook-instagram-813363c8

[5] *Authentication in Internet Banking: A Lesson in Risk Management – Winter 2007 Vol. 4, Issue 2, updated July 10, 2023*. (2023). [Supervisory Insights]. Federal Deposit Insurance Corporation. https://www.fdic.gov/regulations/examinations/supervisory/insights/siwin07/siwinter2007-article05.html

There is no "single point of contact" for fraud reporting in the United States. Instead, reports of fraud are received by five federal agencies, one private non-profit, state Attorneys General, and local law enforcement.[6] The FBI, one of those five federal agencies, has a toll-free fraud reporting hotline. Clearly, an opportunity exists to build and promote a nationwide fraud reporting system.

Support local law enforcement:
Congress should fund state-level financial crime units to disseminate best practices for policing against fraud, provide instructions on fraud reporting, and support more thorough investigations of identity theft, check fraud, forgery, and other payment fraud.

Hold telecoms accountable
Without the ability to send fake text messages and impersonate personal contacts over the phone, it would be much harder for fraudsters to do their work. Telecoms are gatekeepers who are uniquely positioned to thwart the implementation of fraud. They should be required to prevent fake caller ID and address SIM card thefts.

Force Big Tech to clean up its platforms.
By many accounts, social media platforms are central to the execution of fraud. Unfortunately, social media platforms have a vested financial interest in doing business with criminals. They receive revenue from paid posts. According to the FTC, more money is reported lost due to fraud that originated from social media than from any other method of contact.[7]

Platforms must be compelled to remove content when they are aware it has contributed to fraud. It should not be necessary for a platform to receive 30 complaints before it acts. These companies are spending billions of dollars on artificial intelligence. They must have the resources to spot fraud. Congress should update Section 230 of the Communications Act of 1934, enacted as part of the Communications Decency Act of 1996, to remove barriers that permit social media platforms to evade responsibility for criminal activity occurring inside their products.

Additionally, stakeholders should streamline the receipt of complaints to make them more useful. One step would be to create a standardized and ubiquitous system for complaint intake. Reports received from victims should be uniform, with appropriate information coding, to enhance the collection, analysis, and redistribution of fraud complaints. These intake forms could be shared with all institutions that currently accept fraud reports.

Fraud affects everyone: young and old, rural and urban, servicemember and civilian, and in every community across the country.

---

[6] Federal Trade Commission. (2025). *Consumer Sentinel Network Data Book 2024*. https://www.ftc.gov/system/files/ftc_gov/pdf/csn-annual-data-book-2024.pdf

[7] Emma Fletcher. (2023). *Social media: A golden goose for scammers*. Federal Trade Commission. https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2023/10/social-media-golden-goose-scammers

Questions 9 through 15: Regulation and Supervision

Question 9: What potential changes to regulations (apart from the Board's Regulation CC, discussed separately below) could address payment fraud and mitigate the harms from payments fraud to consumers, businesses, and supervised institutions?

In faster payments, receiving depository financial institutions (RDFIs) should share in the liability for funds lost due to fraud.

Preventing fraud in faster payments creates unique challenges. Transfers are irrevocable, and settlement occurs quickly. While standard ACH gives the ODFI several days to request a reversal, no such cushion exists in faster payments. As a result, fraud prevention has to rely on algorithmic analysis of payment patterns and rapid information sharing between networks and financial institutions. These tools require engagement by both banks in a transfer, as well as any intermediaries. These conditions did not exist when Congress passed the Electronic Funds Transfer Act (EFTA). The EFTA was passed almost forty years before the Federal Reserve began to plan to introduce faster payments. It is not surprising that its structure does not match this new type of funds transfer. Now is the time to update the law to fix the disparity.

Because RDFIs are positioned to see critical patterns about accounts that remain out of the originating depository financial institution's (ODFI's) sight, they should share in liability for lost funds.

For example, consider the following sequence of transactions in Table 1 that occurred on an account that was taken over by a criminal. Account takeover (ATO) occurs when the credentials of an account are compromised. EFTA classifies transfers out of a taken-over account as unauthorized. In this scenario, the account holder will not be liable for the losses. However, the consumers who were tricked by the criminal into sending money to this account will not have EFTA protections. Their transfer orders will be considered authorized.

In this version of an ATO scheme, the criminal takes over an account at a bank by stealing sign-in credentials. From there, the criminal convinces five people to send money, under false pretenses, in an imposter scam, to the compromised account on November 14th. Those victims are using other accounts, most likely from different banks. They will be the victims who lose money.

Transactions 9 through 13 are transfers from a different bank into the account that the criminal has taken over. Because other customers authorized those transactions at sending banks, they will be considered to have been authorized. Under current rules for transfers authorized by account holders, the account holders who make transactions 9 through 13 will not have a right to receive their lost money.

After the transfers have been completed, the fraudster quickly pulls funds from the account they took over to other accounts. The money may leave the account at the RDFI in minutes.

Table 1: Ledger of funds transfers in a taken-over account

Number	Date	Action	Debit	Credit	Balance
1	Oct. 1	Starting balance			$1,540
2	Oct. 2	Direct Deposit (work)		$1200	$2,740
3	Oct. 2 to Oct. 15	ATM, debit swipes, ACH, checks, and rent paid by Zelle	$2,150		$590
4	Oct. 16	Direct Deposit (work)		$1,200	$1,790
5	Oct. 16 – Oct. 30	ATM, debit swipes, checks	$ 1,084		$706
6	Oct. 30	Direct Deposit (work)		$1,200	$1,906
7	Oct. 30 - Nov. 13	ATM, debit swipes, ACH, checks, rent paid by Zelle	$1,850		$56
8	Nov. 13	Direct Deposit (work)		$1,200	$1,256
		Account credentials are stolen. The criminal begins to use the account			
9	Morning of Nov. 14	Zelle deposit received. (Sent from a victim)		$88	$1,344
10		Zelle deposit (from a victim)		$4,240	$5,584
11		Zelle deposit (from a victim)		$1,656	$7,240
12		Zelle deposit (from a victim)		$900	$8,140
13		Zelle deposit (from a victim)		$505	$8,645
		Criminal transfers funds received from victims to other bank accounts			
14	Shortly after the deposits post on Nov. 14	Zelle transfer out of RDFI	$1,800		$5,965
15		Zelle transfer out of RDFI	$1,445		$4,520
16		Zelle transfer out of RDFI	$1,990		$2,530
17		Zelle transfer out of RDFI	$1,885		$645
18		Zelle transfer out of RDFI	$269		$376
	Nov. 15	Under network rules, RDFI should file a report to Zelle			
19	Nov. 14-Nov. 16	ATM, debit swipes, checks	$914		$-538
		Notification and account closure			
20	Nov. 14-Nov. 17	Customer incurs overdraft fees	$105		-$643
	Nov. 17	Customer receives first notice of overdrafts by mail			
	Nov. 17	customer complains to their bank (RDFI)			
		Bank considers refunding the overdraft and NSFs			
	Dec. 12	bank files SARs report[8]			

This ledger shows how the RDFI had insight into the unusual account activity occurring on the account.

This fraud could have been prevented if the RDFI had identified the deposits received on Nov. 14th (items 9 through 13), graded them as high-risk, and not credited the proceeds to the compromised account. However, the RDFI released the funds. The criminal quickly transferred those funds out of the account. The RDFI should have noticed that the only deposits to this account are direct deposits for $1,200 from an employer, and the only Zelle transfers going out were to pay rent. The RDFI's response is important – and expediency is critical. The RDFI could have shut the account down on the 14th, or when it filed the fraud

[8] Banks have up to thirty days to file SARs and are not required to issue reports for transactions of less than $5,000, or more than $2,000 if it involves a money service business. At their discretion to they can file reports for smaller transactions.

report to Zelle, or it could have waited until the customer complained several days later. The worst outcome occurs if the RDFI waits until the consumer files a complaint. By then, the funds will have been gone for three days.

Despite the opportunity to hold the funds, the RDFI will not be liable for losses incurred by account holders at ODFIs who sent funds to its account holders. Those account holders will have lost almost $7,389.

The ledger also shows that while mandated information sharing is important, it is essential that it occurs promptly. Under Zelle rules, the RDFI is supposed to file a report within 24 hours. That is helpful – while it would still be too late to recover the funds lost on the 14th, it could help prevent further outflows. Those rules are Zelle's – they are not universal across all other faster payment services, such as those built for commercial firms.

In some instances, the RDFI could have prevented this from happening. If the account was opened using a synthetic identity, then it was the RDFI that failed to fulfill the expectations of "know-your-customer" regulations.

To eliminate any plausible deniability among banks that hesitate to address fraud, the Federal Reserve should issue guidance for Regulation J explicitly stating that RDFIs can refuse to complete a payment order when they believe the transfer would fulfill a fraudulent request.[9] To protect consumers who sent funds, they should clarify that RDFIs should return the funds as soon as possible to the sender, with an explanation.

Criminals exploit banks' poor fraud prevention to access the bank accounts needed to commit crimes. Yet when banks fail to prevent fraud, consumer victims bear the burden.

The Bank Secrecy Act (BSA) penalizes banks for failing to prevent criminals from opening accounts. The regulations are clear that banks must have appropriate know-your-customer (KYC) and customer identification procedures (CIPs) in place. Criminals who engage in scams to convince people to send money under false pretenses often open accounts using false identities. For their work to succeed, it is necessary for a bank to approve them for an account.

Left unaddressed, however, are the outcomes for people who were tricked into sending money to these accounts. The BSA does not address the issues of victims, and EFTA overlooks the complicity of an RDFI that opened the account used by a criminal to receive funds in an induced fraud. Since EFTA does not protect consumers if they authorize those transfers, a victim of an induced fraud is left without recourse, even though it was necessary for a bank to fail to use due diligence in reviewing account opening applications for the crime to have succeeded. This is a gap that should be closed.

The emergence of online banking has expanded the share of applications made over the internet and increased the risk caused by banks with lax security standards. Unfortunately, online accounts are

[9] Reg. J, 12 C.F.R. § 210.44(b)(3).

disproportionately more likely to be the object of fraudulent account applications. In the past few years, many sponsor banks in fintech partnerships have been penalized for non-compliance.[10] Most recently, Evolve Bank & Trust was shown to have permitted scores of accounts to be opened from a single address in Wyoming by applicants with IP addresses in foreign countries, including countries on the Office of Foreign Assets Control list. The scenario in Table 2 shows the status of a set of Evolve accounts that were opened using synthetic identities.

Table 2: List of accounts opened for a fintech partner of Evolve Bank & Trust [11]

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

Evolve Bank & Trust approved these accounts through its partnership with Mercury, a small business fintech company. While many are now closed, they were all active at one point, and all still have balances.

There is a victim – or perhaps many victims – behind each of these accounts. Those accounts may have been used for transferring funds between criminals involved in various illicit activities. It is also possible

[10] S&P Global. (2024, January 23). *Small group of banking-as-a-service banks logs big number of enforcement actions*. 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

[11] Mikula, J. (2024, July 21). Synapse Program Was "Nightmare Fuel" Due To Control Gaps, Ex-Employee Says [Substack newsletter]. *Fintech Business Weekly*. https://fintechbusinessweekly.substack.com/p/synapse-program-was-nightmare-fuel

that these accounts could have been opened by criminals involved in perpetrating imposter scams, investment scams, or other schemes used today to trick people.

Liability should be applied to institutions that can prevent fraud from occurring on their platforms. For its failure to prevent the fraud, prudential regulators should hold the RDFI accountable for non-compliance with the BSA and its implementing regulations. But action must be taken to help consumers who are the downstream victims of compliance failures.

One policy option would be for prudential regulators to include consumer redress when they penalize banks for not complying with BSA laws, particularly when those shortcomings result in consumers being defrauded at ODFIs. Alternatively, Congress could rewrite EFTA, requiring the CFPB to develop rules to assign a portion of liability to RDFIs.

These scenarios should underscore how RDFIs must be brought into the liability framework. When RDFIs fail to protect accounts from being taken over or when they approve applications from criminals, they create the conditions that permit fraud to flourish.

Question 10. The Board, FDIC, and OCC have issued supervisory guidance on numerous topics that relate to payment fraud detection, prevention, and mitigation. Is existing supervisory guidance related to payment fraud sufficient and clear? If not, what new or revised supervisory guidance should the Board, FDIC, and OCC consider issuing on this topic within the respective authorities?

Using their authority under the Bank Service Company Act, prudential regulators should supervise third-party non-bank 'banking-as-a-service' (BaaS) providers that provide essential banking functions to banks and their partners.

The advent of BaaS has given rise to more arrangements where third-party BaaS companies offer services to fintechs who work with bank partners to offer financial services. In some instances, banks provide BaaS services to fintechs, but in other cases, the BaaS provider is unaffiliated with a financial institution. Recently, a BaaS provider not associated with a bank failed to perform several essential components of banking services.[12] Ledgers were compromised, information technology systems were not maintained, and banks could not link deposits to their owners. Some of the mistakes – such as the failure of the bank partner to ensure the BaaS provider could pay its vendors for information technology services – were already stated in the interagency third-party guidance. The guidance was in place, but its compliance was not verified.

The recent problems with BaaS providers underscore the need for ongoing supervision of non-bank BaaS companies. The prudential regulators should supervise these relationships to ensure that all interagency guidance on third-party relationships is being followed.

---

[12] Faridia, O. (2024, July 5). Synapse, MongoDB Data Disagreement Worsens Ongoing Crisis Over Fintech App Users' Funds. *Crowdfund Insider*. https://www.crowdfundinsider.com/2024/07/227226-synapse-mongodb-data-disagreement-worsens-ongoing-crisis-over-fintech-app-users-funds/

Question 11. How might new or revised supervisory guidance assist small community banks in detecting, preventing, and mitigating payment fraud?

All financial institutions, regardless of their size, must prevent fraud from occurring in their lines of business.
Unfortunately, in an ecosystem with more than 8,000 insured depositories, fraud prevention capabilities vary greatly among banks and credit unions. Nonetheless, banks must remain responsible to prevent fraud. They must conduct effective know-your-customer procedures, maintain awareness of patterns, and comply with the rules for the BSA.

Information sharing is an essential tool in building strong defenses against fraud. Because there are costs to sharing information, firms may be reticent to invest in needed technology and staffing. Moreover, because the benefits of fraud information sharing exhibit the characteristics of a "public good," regulators should update EFTA to apply liability for funds lost due to fraud where the consumer was tricked into sending money under false pretenses. In faster payments, where transfers are irrevocable and may settle far before a consumer can alert a bank, liability should be shared between sending and receiving banks.

Unfortunately, some banks will never invest to the level necessary to achieve the maximum collective gain. Prudential regulators must ensure that all banks have built effective defenses. Banks lacking the capacity to build expense risk analytics can hire companies to do so on their behalf. For example, third-party providers exist to offer solutions for identifying high-risk payment patterns (e.g. SardineX) in real time or to provide second-look reviews of higher-risk online bank account applications (e,g, SentiLink).

Question 12. What is the experience of consumers and businesses when supervised institutions place holds on depositors' funds because of suspected payment fraud? (Regulation CC's "reasonable cause to doubt collectability" exception is discussed separately below.)

(a) For instance, how frequently are consumers and businesses affected by holds, delays, or account freezes, and how responsive are supervised institutions to inquiries from consumers and businesses regarding these issues?

(b) Do current disclosure requirements effectively address consumer and business concerns when supervised institutions hold customer funds due to suspected payment fraud? For example, should changes be considered with respect to permissible customer communications under SAR confidentiality rules?

Bank examiners should monitor the policies and procedures of banks to ensure that these systems are designed to prevent fraudulent transfers and illegal account openings, not prevent well-intentioned consumers from accessing financial services.
Complaints about involuntary account closures have increased almost thirtyfold since 2015.[13] Consumers experience significant problems when financial institutions close accounts or place holds on deposits.

[13]Kate Berry. (2025, February 27). How big of a problem is debanking? No one knows for sure. *American Banker*. https://www.americanbanker.com/news/how-big-of-a-problem-is-debanking-no-one-knows-for-sure

Effectively, a bank account is a necessary tool for almost all households today. Households at any level of wealth would be harmed when they cannot access their funds.

Currently, fraud prevention services blur important boundaries. Under the guise of fraud prevention, some companies sell lists of consumers who have outstanding debts to financial institutions. Banks use these lists to assess the suitability of checking account applicants. Those services are not fraud prevention, but debt detection. The people rejected by these services are not fraudsters looking to commit crimes. They are individuals with debts who require a bank account. Accordingly, regulators should be wary of bank practices that are made under the guise of fraud prevention that do not have any meaningful benefit to stop fraud but bar low-wealth households from the banking system.

Adverse action notification is essential.
Consumers deserve to understand why their bank account was closed or if their funds are being held. With credit accounts, consumers have a right to notification if they are denied credit or receive it on less desirable terms. These protections are not in place for bank account holders. Banks should be held accountable to provide a customer with prompt notification with an explanation when their account is closed or frozen. Timeliness is crucial, as the impact of an adverse event is felt immediately. Therefore, an explanation should occur as quickly as possible, ideally within two business days. Account holders should have the right to contest the decision.

Too often, poor fraud detection systems exclude the wrong people from the banking system. It is already hard enough for many people to get accounts – particularly if they lack the needed indicia – and it would be much worse if policy reaffirmed those problems.

Questions 16 – 20: Payments Fraud Data Collection and Information Sharing

Question 16. Broadly, how could payment fraud data collection and information sharing be improved?

Financial institutions should do more to share information with other financial institutions. Sharing information across a transaction is essential. Industry-led reports have stated that more sharing of information on a timely and ongoing basis among a consortium of collaborating financial institutions would further advance fraud prevention efforts.

One hurdle to overcome lies with the financial institutions – mostly the largest banks – that are hesitant to share data when they perceive they have proprietary advantages over their competitors. Many large banks have robust "fraud engines;" too often, others do not. Ultimately, banks that cannot invest in proprietary anti-fraud technology must hire third-party service providers. Fraud prevention should be perceived as a cost of doing business. Regulators should not "tailor" light fraud prevention requirements for smaller institutions.

Financial institutions cannot share fraud information solely at their discretion. Information sharing – and the use of information received as a result – should be mandatory. In faster payments, Early Warning Services (EWS) has required financial institutions participating in Zelle to contribute to and use their

fraud prevention tool. Although EWS launched Zelle in 2017, Risk Insights, its fraud prevention software overlay, was not initiated until 2023. It is one of several network policy changes that may contribute to lower rates of fraud on their platform. As stakeholders involved in facilitating the exchange of real-time payment information, EWS is positioned to implement this approach. Networks in other payment systems should implement similar requirements. Notably, these requirements should be mandatory, not discretionary, and should come with penalties for non-compliance.

Better coordination between law enforcement agencies could improve the collection and analysis of fraud reporting.
The FTC, the CFPB, the Federal Bureau of Investigation, state Attorneys General, federal prudential banking regulators, the Better Business Bureau, the US Department of Education, and local law enforcement agencies all collect fraud reports from victims.[14] All of these entities should collaborate to fight fraud.

Question 18: What role should the FRS, FDIC, or OCC take in supporting further standardization of payment fraud data? For instance, can the FRS better leverage or improve the FraudClassifierSM and ScamClassifierSM models?

Operators – including the Federal Reserve - are well-positioned to prevent fraud, but they need to enhance their information-sharing processes.
Operators should not exist in silos. Significant improvements would be made if real-time payment providers like FedNow and The Clearing House RTP coordinated more closely. Even modest steps—such as adopting standardized fraud reporting codes—would yield meaningful benefits.

Operators should share information between ACH, wire, and faster payment systems.
Today, even information sharing across different Federal Reserve payment systems is fragmented. Fedwire and FedNow are implementing ISO 20022 messaging standards, which can hold 10 megabytes of data, but FedACH uses the traditional NACHA 94-character ASCII text format. ISO 20022 can support detailed messaging information in ways that older formats cannot. [15]

Sharing information between operators working within the same payment rail is insufficient. Cross-rail sharing should also occur. To do that, methods for sharing information should be made as consistent as possible across payment rail systems. For example, fraud reporting codes should be uniform to the extent possible across all systems. Logically, if a bank detects fraud occurring in ACH transfers to a bank account and relays the information back to the relevant operator, the faster payment and wire operators should be alerted as soon as possible, and vice versa.

---

[14] Federal Trade Commission. (2025). *Consumer Sentinel Network Data Book 2024*. https://www.ftc.gov/system/files/ftc_gov/pdf/csn-annual-data-book-2024.pdf

[15] Federal Reserve. (n.d.). ISO 20022 Messages Overview. *FedNow Readiness Guide*. https://explore.fednow.org/resources/readiness-guide-iso-20022.pdf

Question 19. What types of payment fraud data, if available, would have the largest impact on addressing payment fraud? If these data are not currently being collected or shared, what entities are best positioned to collect and share such data?

The FTC is the leading provider of public fraud reporting. Updated regularly, with data received from many different agencies, the Consumer Sentinel Network (CSN) reports and data tools are the best resources available to understand trends in fraud and scams.

Nonetheless, the data should be updated to make use of the more granular information that is being collected with the Federal Reserve's ScamClassifier tool. The ScamClassifier reveals the type of event that led an account holder to authorize a transaction that led to fraud.

- In authorized transfers, reports should distinguish between first-party fraud and relationship or trust fraud. Clarifying the difference is incredibly important, as the implications for remedies are almost the opposite.
- It should disaggregate payment app fraud between non-bank ACH payment apps (Venmo, PayPal, etc.) and bank faster payment apps.
- It should reveal what percentage of complaints were resolved with a financial remedy.
- It should provide data on the number of involuntary account closures that occurred due to fraud.

The CFPB published information on the experience of servicemembers impacted by payment app fraud in 2022.[16] The CSN provides a Tableau-generated table with data points on fraud complaints from servicemembers.[17] These are helpful, but not enough. As a result of legislation passed this spring, the CFPB will not be able to conduct supervision on payment apps. The FTC should expand reporting on this subject to include detailed information on how fraud is affecting servicemembers at a frequent cadence.

Question 20: Is there a need for centralized databases or repositories for the sharing of payment fraud data across entities? What legal, privacy, or practical risks and challenges could such a centralized database or repository pose? Which entities are best positioned to develop and participate in a centralized database or repository?

Solutions to prevent fraud in faster payments require near-immediate response times. A central government-managed repository can help, but it cannot be the only place where information is shared. While some financial institutions have called on regulators to establish a centralized public repository for fraud information, such an effort may not be effective for faster payment systems. Faster payments post almost immediately and can be settled soon thereafter. Fraudsters will have transferred funds out of the account at the RDFI well before data can be made accessible inside a repository.

---

[16] Consumer Financial Protection Bureau. (2023). *Office of Servicemember Affairs Annual Report 2022*. https://files.consumerfinance.gov/f/documents/cfpb_osa-annual-report_2022.pdf

[17] Federal Trade Commission. (2025, March 7). *Military Reports: Reports from Active Duty Servicemembers 2020 to Present*. Tableau Public. https://public.tableau.com/app/profile/federal.trade.commission/viz/MilitaryReports/Infographic

In faster payments, a centralized government-led repository would likely be too slow to have an effect on fraud prevention in real-time. It would be less responsive than fraud information-sharing mechanisms embedded within the networks and operators of these payment systems. Moreover, creating an external repository could unintentionally shift responsibility away from the faster payment networks, which are best positioned to detect and act on fraud due to their direct, real-time visibility into transactions.

At the same time, even if faster payment systems present a unique set of challenges, a repository would have positive effects in other parts of the payment ecosystem. The call for more collaboration between operators, networks, and financial institutions should be supported through a common repository. A repository that connects ACH with faster payment and wires, using common reporting codes and messaging standards, would have positive effects. Additionally, a repository should become the destination for a "single point of contact" for fraud reporting.

Conclusion

Thank you for the opportunity to comment on these important questions. Changing how EFTA and its implementing regulations interpret induced fraud is a foundational step. Not only should banks have liability for funds lost due to induced fraud, but the responsibility should be shared between RDFIs and ODFIs. Wherever possible, regulators should use their enforcement powers to hold financial companies accountable for unsafe financial products. Other steps – many of which are technical or administrative – can strengthen defenses against the work of malicious actors.

Please contact me at [redacted] for any clarifications or to consider additional questions.

Sincerely,

[redacted]

Adam Rust
Director of Financial Services
Consumer Federation of America