September 15, 2025

https://www.regulations.gov

Re: Request for Information on Potential Actions to Address Payments Fraud (OCC Docket ID OCC-2025-0009, FRS Docket No. OP-1866, FDIC RIN 3064-ZA49)

Dear Federal Reserve System ("FRS"), Office of the Comptroller of the Currency ("OCC"), and the Federal Depositors Insurance Company ("FDIC"),

BAFT (Bankers Association for Finance and Trade) welcomes the opportunity to respond to the Request for Information ("RFI") on Potential Actions to Address Payments Fraud, which was published in July 2025.

BAFT is an international financial services industry association whose membership includes U.S. banks which range in asset size from G-SIBs to Regional Banks with less than $20 billion in assets, as well as a broad range of other financial institutions throughout the global community, many of which also operate within the United States. As a worldwide forum for analysis, discussion, and advocacy in international financial services, BAFT member banks provide leadership to build consensus in preserving the safe and efficient conduct of the financial system worldwide. BAFT closely monitors the impact that new regulatory initiatives could have on the provision of payment services and trade finance that support real economic commerce.

BAFT's key positions regarding the RFI, as detailed in this response, are as follows:

1. What actions could increase collaboration among stakeholders to address payments fraud?

Collaboration should be as wide as possible both in terms of industry and geographic reach. US financial institutions play an important role in preventing fraud, but coordination with other industries is required. Furthermore, fraud is not a United States specific problem, so it seems reasonable to work internationally to combat fraud.

Across domestic and international stakeholders, such regular industry engagements with regulators can facilitate the sharing of best practices in fraud prevention, and the latest payment fraud trends observed by industry stakeholders. For instance, the use of payment tokenization can be encouraged to minimize exposure of sensitive transaction-related data.

A requirement should be made to share detailed non-card fraud payment data across the industry. It should be separated by retail/consumer and commercial, with an ability to cross over segments for best practices development. Industry benchmarking - especially for entity/commercial accounts - is needed.

There is a need for near real time fraud information sharing and red flags. This timeliness issue impacts the ability of a bank to detect and prevent fraud within its own walls and across financial institutions (FIs). This would aid in 'breaking the chain' of fraudulent money movement. Shared data should consist of transactional data (i.e. account level data) as well as other relevant identifiers (i.e. device IDs, IPs, bad bene info, etc.). Such information should be utilized to feed standard fraud detection services and systems used for real time and near real time decisioning (much of it is done in batches today).

Clearly defined responsibility and liabilities by all banks - broken down by issuing bank, vs. bank of first deposit (BOFD), etc., should also be established. Standards need to be developed for payment solutions outside of banking (i.e., Cash app, PayPal, Plaid, Venmo, etc.), to which they are responsible to support a safe and secure operating environment and are responsible when their tools are used in fraudulent transactions.

Cross-agency collaboration should be required, with the support of cross-industry efforts (social media, telecoms, etc.) to work with banking institutions, as fraud often commences first outside of the transaction itself. Identification of mule accounts, fake social media used for data collection, scam proliferation, etc., should be made a priority. Collaboration with FinTechs would also be needed in the stakeholder group to develop a practical and useful solution. FinTechs would have to specifically support banking regulations and should be held to similar regulatory standards as banks.

A. Ability to verify account ownership, funds availability across FIs
B. Standardize notification and recovery process to recover losses for the customer and the bank

A stakeholder that has been seldom discussed is the precious metals industry. There are more cases of criminals moving the proceeds of their activity to a precious metal company. Consideration should be given to what type of authentication and due diligence they do prior to the release of the funds.

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

Depending on the type of fraud involved (authorized vs unauthorized) and which role the FI plays (ordering, intermediary, or beneficiary), amongst other things, should determine the preventative measures which an FI should implement, which would mitigate the respective risk. Guidance against perceived weaknesses could be an effective way to address payment fraud but should be coordinated to the extent that they are applicable to the various FIs which all possess such potential weakness. For example, if two-factor authentication prevents hacked accounts[1], guidance should be coordinated to the extent appropriate.

It is worth remembering, however, that criminals are adaptable. For instance, even if Confirmation of Payee is implemented to help tackle authorized push payment fraud, fraudsters can adapt by making sure the name they provide to the victim is the name of the account

[1] Two-factor authentication analysis: https://consumer.ftc.gov/articles/use-two-factor-authentication-protect-your-accounts

holder.[2] Therefore, any guidance should be analyzed to determine its actual effectiveness, which may require offering several alternative points for comparison.

The employment of industry standards such as the Payment Card Industry Data Security Standard (PCI DSS) will mandate network participants' commitment to fraud prevention and data security.

Every communication channel has its own distinct exposure to fraud risk. Deploying multi-factor authentication via more secure channels can reduce the incidence of fraud. For example, push notifications in a verified app occur within a closed-loop environment and can be encrypted as additional layers of security, compared to methods like SMS, which run the risk of having sender labels spoofed by malicious actors.

A transaction risk scoring standard can also help provide payment processing institutions with an indicative transaction risk profile. Modelling a parameterized risk profile based on the details of the transaction origination, with industry standard guidance on high/medium/low risk scoring ranges, leverages network-wide data and provides a more holistic view of the transaction. Such a risk score can be used to trigger corresponding risk mitigation strategies, such as requiring callback, dual transaction approval control, or multifactor authorization where appropriate.

The efficacy of a uniformly applied industry standard hinges on the commitment of industry players to full adoption. A possible hurdle would be obtaining alignment across industry participants on the standards to be prescribed due to the varying risk appetites of each organization.

Alternatively, there can be the provision of industry best practices which are non-binding but function as guidance for financial institutions to assess their existing processes. For example, if nationally-aggregated data points to the use of hyperlinks as a high-risk factor for payment fraud, financial institutions may be discouraged from using hyperlinks in their digital communications to customers.

There is a lack of consortium groups in general. For strong groups like ABA and BITS, support of the lobbyists representing banks is also lacking.

A requirement should be made to share non-card fraud payment data across the industry. It should be separated by retail/consumer and commercial with an ability to cross over segments for best practices development. Industry benchmarking - especially for entity/commercial accounts is needed.

Non-card fraud commercial consortium groups are lacking - this is important as the onboarding process and commercial client actions are materially different than a retail client with potentially different solutions and client management requirements.

There is a need for near real-time fraud information sharing and red flags. This timeliness issue impacts the ability of a bank to detect and prevent fraud within its own walls and across FIs. This would aid in 'breaking the chain' of fraudulent money movement. Shared data should consist of transactional data (i.e. account level data) as well as other relevant identifiers (i.e. device IDs, IPs, bad bene info, etc.). Such information should be utilized to feed standard fraud

[2] BAFT response on FATF R16: https://www.baft.org/policy-news/baft-comment-letter-to-fatfs-second-public-consultation-on-payment-transparency-proposed-revision-to-r-16/

detection services and systems used for real time and near real time decisioning (much done in batch today).

Collaboration, connection, and support among key stakeholders is necessary, including law enforcement, CFPB, FTC, FCC, Homeland Security, Postal Inspection, and other industry private sector participants (telecom, social media, fintech's).

Also, the notification should be standardized. The biggest obstacle today is in establishing contact and reporting fraud between financial institutions.

Consumers would benefit from FIs, Telcos, and social media companies collaborating to address the entry point of the criminal to the consumer. The ability to establish a standardized foundation to address the criminal's ability to gain access to consumers would be beneficial. Developing an effective authentication/validation process for people to gain access to the ability to create social media that discusses regulated industries such as investments would limit the criminal element offering fake investments to consumers. Social media/Telco companies should have a "know your merchant/seller/user" process, just as banks have a know your customer requirement. The Telco industry needs more stringent standards, an example of which would include that a Telco provider should be the only entity that is allowed to "modify" the name the consumer sees on their caller ID. The ability to spoof a phone number has limited professional benefits and by restricting this type of action to the Telco provider would safeguard consumers. Additionally, phone calls that originate outside of the US should be clearly identified in the caller ID process. The ability for anyone to be able to show a foreign number or a call that originates outside of the US as a US originated call is a deceptive practice and further perpetrates a falsehood to the consumer leading them to be more likely to trust the caller identification and requests. All industries should have the following:

A. A set standard time frame to remove suspicious users from their platform, the creation of a set time frame is set by the sheer volume of criminal activity being perpetrated by these users.
B. A national registry that clearly shows those involved in scams that would allow all industries to inquire into it to allow another data element to work with clients to evidence that they have been targeted for a scam or criminal act.
C. Active processes to identify those insiders that have compromised data or misused a position of trust with a consumer.
D. Social media companies should have active processes that remove content that allows criminal acts to occur i.e. any videos and trainings that show how to get away with scams, manipulate a system for personal gain, how to chemically alter checks, etc.
E. Create a standardized process that allows all stakeholders to share their data in a way that provides a resource to their peers.
F. A process to properly authenticate their client when changes are made to the services provided i.e. port a phone number or port the ability to receive texts from a land or VOIP line. The fact that service providers can do this with a simple copy of a phone bill is unacceptable. A more robust authentication process must exist especially for non-face to face changes made to consumer's communication channels.
G. The ability for FIs and other key stakeholders to be able to properly understand electronic payment origination sources, especially when payment instructions or account

access is seen coming in through a VPN or other tool that allows the true origination site to be hidden.

H. Consideration of the standardization of the intended recipient name on outgoing payments so that the receiver of the funds can appropriately validate that not only is the account number but that the name also aligns to the sender's intended recipient. This would also tie into the technology of being able to inquire into an account name at another FI prior to sending a wire for a consumer.
I. Improved standards on the quality of the check image. Often the quality of the image limits the bank's ability to properly compare the image to historical items.
J. Consideration of incentives to all banks to require their corporate clients of a certain size or check issuance volume to use Payee Positive Pay. This will encourage the transition to a paperless society and will reduce the overall risk of mail theft which will further reduce the risk to postal employees and reduce the volume of altered and forged endorsement claims that are currently creating undue hardship to many FIs who are not able to respond to claims in a timely manner.
K. The creation of a state/federal database that would allow FIs to authenticate the client's identification ideally with the photo on file.
L. Expediated funding for the US Postal system to improve their processes which will lead to a reduction in mail theft and check fraud.
M. Check vendors (printed) should be required to authenticate the ownership and address of the account holder prior to shipment with the FI.
N. Collaboration to establish a consumer reporting standard for those who actively participate in scams or consistently commit 1st party fraud on their deposit account.

3. Which organizations outside of the payments or banking industry might provide additional insights related to payments fraud and be effective collaborators in detecting, preventing, and mitigating payments fraud?

To holistically tackle fraud, particularly authorized fraudulent payments involving some form of manipulation, how the fraudster communicates with the victim should be part of the solution. FTC data shows that most reported fraud occurs through non-face-to-face means (e.g., email, text, phone, websites, social media, or online ads).[3] The providers of these services are best positioned to intercept a fraudster before a payment is even initiated and should therefore be collaborators.

Additionally, many forms of fraud involve the creation of fake documents, such as synthetic IDs[4], or in other cases, deepfakes.[5] Therefore it also seems reasonable to include entities which enable the means to create such fake documents.

Given the global nature of payments fraud, organizations that can identify organized crime which enable payment fraud, both locally and internationally, should be collaborating closely

---

[3]FTC Data: https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudReports/SubcategoryPaymentContact

[4] NCUA on synthetic IDs: https://ncua.gov/newsroom/ncua-report/2018/synthetic-identities-are-one-fastest-growing-forms-identity-theft

[5] Deepfakes: https://www.fincen.gov/news/news-releases/fincen-issues-alert-fraud-schemes-involving-deepfake-media-targeting-financial

with the payments industry. For example, phishing operations can be run out of multiple locales transnationally. Once sensitive information has been obtained from scam victims, there is the potential for payment fraud to occur.

Agree with column F: Law enforcement, CFPB, FTC, FCC, Homeland Security, Postal Inspection and other industry private sector participants (telecom, social media, fintech's) as well including government agencies such as US Treasury, Federal Trade Commission, FCC etc.

4. Could increased collaboration among Federal and State agencies help detect, prevent, and mitigate payments fraud? If so, how?

Yes, it is reasonable that increased collaboration would help combat fraud. For instance, if Regulator A issues guidance on how to combat fraud, but Regulator B does not, then unless there is an intrinsic reason that entities under Regulator B would not need it, fraudsters could perceive entities under Regulator B as having a weakness which can be exploited.

Promoting data sharing by state agencies to federal agencies for consolidation, and access to federal-level data by state agencies can allow for fraud patterns and threats to be identified earlier and more accurately. In addition, the provision of federal guidance or regulation to standardize fraud reporting requirements can reduce information friction provided by organizations operating at the state and/or national levels.

Yes, there should be standardized process to verify and return Federal and State funds. Additionally, there must be a way to locate contacts within the agencies that can be notified in situations involving Federal or State funds.

Maintaining and providing access to a federal central database of bad actors can help counteract bad actors who relocate between states for a 'clean slate' risk profile, evade law enforcement, or exploit differences in state regulatory environments.

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

Typically, interactive learning and engagement tends to help build skills related to specific topics. When it comes to payments fraud education, interactive learning would be a good setting for attendees to learn with a hands-on approach. In addition to interactive settings, real-life scenarios through case studies as a practical exercise would be beneficial for those in the industry aiming to prevent payments fraud from occurring. Tailored training to the audience will pinpoint areas of focus, however, the more involvement and engagement from consumers, businesses, financial crime professionals, and law enforcement, the more comprehensive and effective the output.

Nudges are most often the most effective type of education. We see it a lot in mobile banking applications where consumers will be prompted upon login to be aware of scam/fraud and that bank employees will not ask for certain information.

Yes, payment fraud education must be catered to the audiences, and further, the types of frauds that commonly happen need to be considered. as the educational material would be very different.

Effective Approaches include:

A. **Scenario-Based Learning:** Real-life examples and phishing simulations resonate strongly with both consumers and businesses.
B. **Microlearning:** Short, digestible, and engaging content (e.g., social media stories, gamified lessons, etc.) increases retention and accessibility.

Audience-Specific Content:

A. **Consumers:** Simplified, fun, and relatable content (e.g., Reddit-style stories, influencer-led campaigns).
B. **Businesses:** Targeted education based on industry and payment behavior, including internal control recommendations and fraud-specific risk assessments.
C. **Employees:** Training on how to identify, and effectively communicate and respond to suspected fraud, with a focus on scam typologies rather than payment methods.

Why It Works: These methods align with how different demographics consume information and reflect the evolving nature of fraud, especially among younger audiences targeted via social media.

Banks are very active in providing awareness messages to their clients. Many banks utilize newsletters, inbound call messages, website banners, front line staff etc., to raise awareness.

The most impactful messaging would include a national coordinated campaign by the Federal Government with messaging within the social media platforms that are often where the scammers are finding their targets. Additionally, consideration should be given to a national campaign with several celebrity spokespersons that appeal to the target demographic. It is further recommended that additional mediums be explored, i.e., roundtables, seminars, emails, billboards, advertisements, flyers, posters, federal and state offices as well as currency exchanges and retail environments, especially those selling gift cards. Many of these locations have a wider reach and could send out or display some of this education material for consumers. Fraud and scam awareness would also be very beneficial to the homeless and lower income areas as they are often targeted by criminal groups for recruitment.

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

Absolutely. Additional education regarding safe payment practices will promote awareness for the consumer as well as provide the consumer with what to look for and how to keep themselves safe, and is paramount to mitigating payments fraud. Increasing awareness of safe payment options and processes will help decrease the exposure to payments fraud risks and allows both consumers and businesses to protect themselves.

A. Increased awareness of the potential ways perpetrators commit payments fraud
B. Understanding secure payment methods and options for the consumer
C. Importance of protecting personal information

D. Awareness on how to recognize potential payment fraud risk and who/how to report it

It is important to note that the delivery channel matters as much as the content. It must be relatable as well as memorable. For corporate staff, simulated phishing emails are most often effective in ensuring that employees are aware and alert. For consumers, it would require reminder at friction points.

Yes, additional education is critical.

A. Microlearning and "What to do if scammed" content can reduce fraud initiation and operational burdens.
B. As GenAI accelerates scam sophistication, proactive education is essential to keep consumers informed and vigilant. Education can no longer pull content that people only go to after they have been scammed. We need to push the content as preventative public safety announcements.

Yes, a national campaign to drive acceptance of electronic methods for payments to remove the dependency on checks and the mail system tied to fraud/scam awareness would be beneficial. Additionally, checks are often intercepted that are payable to the treasury for various reasons. Consumers often write checks as they are more comfortable with a paper check "receipt". The inclusion of the most popular treasury accounts within a bank's bill pay platforms would further reduce the dependency on check and yet allow the customer to feel more comfortable with the payment. The messaging of the educational campaigns must be done on multiple layers including at the post office (cut down on money order fraud), billboards, TV, radio and in avenues that will educate the consumer who doesn't have a permanent home or resources don't meet their monthly needs as they are additionally at risk for recruitment into negotiating stolen and fraudulent checks. All types of businesses, from small to large, also need awareness campaigns within their staff, especially in accounts payable areas. While banks execute targeted campaigns, more needs to be done to stop the BEC and payment diversion scams that occur on a daily basis to countless businesses. In some cases, the losses can cause a company to close.

7. Which approaches could make existing payments fraud education more effective? For example, would targeting outreach to particular audiences or conducting additional education in collaboration with other key stakeholders be effective?

Yes, the more coordination and outreach, the more awareness is spread. If regulatory bodies and/or government agencies are able to lead the initiatives applicable and relevant to their local laws to the key stakeholders, that would be most beneficial.

Country-wide campaigns organized by regulators or government would be the most effective, but execution might be difficult. Usage of social media would ensure that education is able to reach masses in a more effective manner, especially usage of short form content.

8. Are current online resources effective in providing education on payments fraud? If not, how could they be improved?

Due to the evolving methods being used to commit fraud, there is a need for more effective resources related to education and awareness on payments fraud. Fraud continues to remain

prevalent in the industry, and continued awareness and education is a key component to combatting payments fraud. Due to new techniques and forms of committing fraud, such as digitization and AI, it is important for the industry to provide dynamic education and best practices for detecting and preventing such threats.

Most practitioners do not actively seek such information online, moreover those that do the research might have already fallen victim to fraud. These resources must be more actively presented to consumers or intended audiences, acting as reminders and warnings.

Current resources are largely ineffective.

Challenges:

A. Lack of awareness and relevance to users' situations.
B. Content is often dry, generic, and not actionable.

Improvements needed:

A. Real-life examples and phishing simulations.
B. Ongoing microlearning beyond onboarding.
C. Use of popular platforms and formats (e.g., short videos, interactive content).

Yes but this is limited to specific age groups. Offline resources must be engaged in greater capacity. The online resources are effective when the site or message captures their attention. The challenge becomes customers normally look for the information after something has occurred. The inclusion of a national campaign that promotes the sites for additional information would be beneficial.

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

Payments fraud involving scams, particularly authorized push payment (APP) scams, business email compromise (BEC), and other social engineering schemes, have become a significant challenge for consumers, businesses, and financial institutions. Unlike unauthorized transactions, scams typically involve victims voluntarily initiating payments under false pretenses, leaving banks and payment providers with limited recourse under current regulations.

To better address this risk, we recommend that the Federal Reserve consider a regulatory framework that draws on FINRA Rule 2165 ("Financial Exploitation of Specified Adults") to establish a safe harbor for financial institutions that take proactive measures to delay or block suspicious payments to protect customers.

I. Leveraging FINRA Rule 2165 for Scam Prevention

FINRA Rule 2165 provides broker-dealers with a safe harbor when temporarily holding or disbursing funds to protect vulnerable customers from financial exploitation. A similar rule for banks and payment service providers could allow institutions to:

A. Temporarily pause or delay suspicious transactions (e.g., wire transfers or real-time payments) when there is a reasonable belief that a customer is being scammed, without incurring regulatory or legal liability for non-completion of the payment.

B. Engage in customer outreach (e.g., contacting the customer or their trusted contact) during the hold period to verify the legitimacy of the payment and provide fraud education.

C. Use fraud signals or behavioral indicators (e.g., sudden large transfers to unknown recipients, transfers initiated under duress) as the basis for temporary holds.

II. Encouraging Proactive Measures with Safe Harbor Protection

A safe harbor, like FINRA Rule 2165, would enable banks to act more decisively and proactively, knowing they are protected when intervening to prevent potential scams. Currently, many banks are hesitant to block or delay transactions due to fears of liability, customer dissatisfaction, or reputational harm, such as accusations of wrongful interference.

Safe harbor protection would incentivize banks to:

A. Enhance real-time fraud detection by investing in AI-based monitoring systems to flag high-risk payments in seconds.

B. Expand scam prevention training for frontline employees and fraud teams to recognize scam behaviors (e.g., romance or investment scams) and intervene effectively.

C. Collaborate across institutions by participating in shared industry databases for mule accounts and scam typologies, enabling early interdiction.

D. Develop customer trust programs that offer customers the option to opt-in for "enhanced scam protection," where payments flagged as high-risk could be delayed for review.

III. Expected Benefits:

A. Reduced scam losses by enabling temporary holds that disrupt fraud schemes.

B. Consumer protection with transparency, as customers are informed about potential scams before their funds are irretrievably transferred.

C. Regulatory clarity through a well-defined safe harbor rule that balances consumer protection with innovation in payment systems.

We encourage the Federal Reserve to consider adopting a safe harbor model, like FINRA Rule 2165, to empower banks and payment providers to take proactive steps against scams without fear of liability, while also enhancing consumer protection and industry collaboration.

Requirement (not encouragement) of the shared responsibilities of controls - including levels of authentication - should be specifically defined. For example, consumers and entities must have

multi-factor authentication enabled along with embedded fraud preventing services, while banks have the capability to receive information and act in real-time/near real-time in the decisioning and accepting of payments.

Regulatory agencies should shift their supervisory approach toward a results-based review of financial institutions, rather than focusing solely on strict adherence to policies. Fraud and scam trends evolve rapidly, and regulators need to keep pace—allowing financial institutions to make risk-based decisions without fear of penalties for not following every policy to the letter. What matters most is the outcome for consumers and the financial system, not whether a box was checked.

Examinations should therefore emphasize results, including the effectiveness of fraud prevention efforts, the volume and value of scams stopped, and the timeliness of issue resolution. At the same time, some existing regulations are outdated and do not reflect today's digital environment, where scams pose one of the greatest risks to consumers.

Given that consumers are losing record sums, regulations across industries must be updated. Banks in particular need greater latitude and safe harbor protections to stop authorized transactions that are clearly the result of scams. When acting in good faith, banks should be able to deny transactions or temporarily block accounts until trusted contacts or protective services can be engaged—while still ensuring that valid consumer transactions are processed without undue disruption.

It would also be beneficial for the financial services community for examiners to share their insights with the community - fostering a more open, cohesive and proactive environment. The sharing of information would allow peer banks to see what trends they have identified so they can proactively address that risk, share systemic issues so that all users of a system can address the gap timely to reduce downstream impacts. The regulatory agencies should work with their peers to ensure exams are not repetitive in nature and are done in a way that is not taking away resources from their fraud prevention duties for extended periods at a time. Additionally, the agency should consider the impact to the FIs team while working on the exam to properly be able to manage their fraud risk and be responsive to frauds in progress and new evolving trends.

10. The Board, FDIC, and OCC have issued supervisory guidance on numerous topics that relate to payments fraud detection, prevention, and mitigation. Is existing supervisory guidance related to payments 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?

While the guidance is clear, the ability of banks to implement the guidance requires investment. Differing interpretations of the guidance lead to different implementations, varying from bank to bank, and, as a result, does not create a cohesive ecosystem for fraud detection, prevention, and mitigation. We recommend that regulators can do the following to mitigate this variation in implementation:

A. **Standardized Implementation Frameworks**

- Provide clear supervisory expectations, templates, or minimum control standards to reduce room for interpretation.

- Example: Standard fraud reporting formats or risk-scoring methodologies.

B. **Safe Harbor Provisions**

- Offer legal or regulatory protection for banks that act in good faith when applying guidance, even if their methods differ.
- Encourage proactive fraud prevention without fear of penalties.

C. **Industry Coordination & Knowledge-Sharing**

- Facilitate cross-bank forums or working groups to align best practices and reduce inconsistencies.
- Encourage joint development of fraud typologies and detection models.

D. **Regulatory Sandboxes & Pilot Programs**

- Allow banks to test innovative fraud prevention methods under regulatory oversight.
- Provide feedback loops to refine guidance and encourage scalable solutions.

E. **Clearer Cost–Benefit Alignment**

- Recognize the resource investment required and provide phased implementation timelines, proportional requirements for smaller institutions, or incentive structures (e.g., reduced reporting burdens for early adopters).

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

"Too often, bankers focus purely on the laws and regulations without appropriate regard for, or knowledge of, the specific purpose for which they were created. Without an understanding of the risks they were designed to mitigate, it is extremely difficult to ensure they are interpreted and applied correctly."[6]

Supervisory guidance could provide tailored risk assessment tools that specifically address the unique challenges faced by smaller institutions, such as limited resources and staff expertise, to assist them implement effective fraud risk management programs proportional to their size and complexity. Clear guidance on prioritizing risks based on new accounts, transaction volumes, customer base characteristics, and local market conditions would be particularly valuable.

New guidance can provide clearer and simplified expectations regarding fraud risk assessments, control activities, and ongoing monitoring for community banks to understand and fulfill regulatory requirements.

[6] Claravall, Tadeo, 2021 - Financial Crime Fighter - Book of Mentors: Practical Career Advice From Leaders In Our Profession. Published by The Financial Crimes Haymarket

Guidance can encourage and establish mechanisms for information sharing between community banks, peer financial institutions, industry stakeholders, and law enforcement, enabling them to collectively combat evolving fraud threats.

Many community banks struggle with knowing which fraud prevention technologies are the most effective for their size. Supervisory guidance could outline minimum technology standards, provide vendor evaluation criteria, and suggest implementation timelines that are achievable for smaller institutions. This might include guidance on machine learning tools, transaction monitoring systems, and customer authentication methods.

Guidance could establish standardized training programs for fraud detection, assisting community banks to develop internal expertise. The guidance could suggest certification programs, regular training modules, and knowledge-sharing networks among community banks to pool resources and expertise.

Clear guidance on customer education requirements could help community banks implement consistent fraud awareness programs. This is particularly important since community banks have closer customer relationships and can be more effective at direct education efforts.

Streamlined incident response procedures bespoke to community bank capabilities would help ensure prompt action when fraud occurs. This would include clear escalation procedures, reporting requirements, and recovery processes.

Overall, revised guidance could ensure that fraud prevention requirements are appropriately scaled to community bank operations, avoiding one-size-fits-all approaches that may be designed for large institutions. This includes clarifying expectations for due diligence, monitoring thresholds, and documentation requirements.

Smaller banks have lesser resources to implement fraud mitigation efforts. Additional guidance would help smaller banks determine where to focus their limited resources to migrate the most risk. Additionally, the recommendation above for exam agencies to share outcomes and trends will further assist all banks in becoming stronger and more proactive.

Smaller banks must be encouraged to become engaged with their industry peers to be able to share fraud prevention knowledge, trends and technology. Currently, while some small banks are very active in the prevention community on a national level, others only collaborate within their local area, missing out on the opportunity to learn from their larger peers and to build those connections to stop fraud in progress by having a contact at the bank who can be responsive. Fraud is not a competitive industry, it would be positive for the regulators to encourage larger national groups to allow smaller banks to join their association at significantly discounted rates or for free or allow them to join select fraud prevention calls so that the knowledge of the industry can be shared. This is similar to when legal firms offer pro-bono work, and incentives should be offered to the group to allow for a more inclusive fraud prevention environment.

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

Investment in operating systems and connecting fraud systems with appropriate models (with consortium data sharing) would theoretically reduce the false positive in identifying risky payments and in theory reduce the number of items held, and have a positive impact on clients.

This may be more relevant in the retail/consumer space.

Customers who have a Reg CC hold placed on a deposited item are dissatisfied. The creation of additional data sharing tools between FIs would reduce the volume of false positives which impact the customers. This would allow for focus on the highest risk items where extended holds availability is needed for more in-depth review to reduce the potential loss to the consumer and/or the bank. Additionally, in some situations the check hold time under Reg CC isn't long enough and the item is then returned causing a debit to the client's account. The client is then impacted when the return is posted causing other payment instructions issued by the client to be denied(returned) causing additional customer dissatisfaction with the financial services community. It should be also noted that clients often view the removal of a Reg CC hold as proof that the check has cleared and has no potential of being returned in the future. However, with the time it takes to return items through the standard process and the extended time it takes for breach of warranty claims to be processed this is often not the case.

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?

For business clients, the experience can be as follows: once there is suspected fraud, the account is placed on restraint. The account is in a pay or no pay status. Emails are sent to clients each day until the client decides to 1) open a new account or 2) implement one of the bank fraud prevention services (i.e., Positive Pay, check block, etc.). Prior to the banks' offering fraud prevention services, the client would often be impacted by holds, delays, or account freezes. Since the onset of fraud prevention services, instances have declined.

We address any concerns our clients bring to our attention regarding Reg CC holds or accounts promptly to ensure a positive customer experience. However, there are times where we are dependent on another FI for information that can help determine the risk of the item being returned or the customer being targeted for a scam. The industry's concern around the ability to release information as discussed above causes delays in our ability to service the customer promptly in some situations. Additionally, in many cases customers don't understand that they have the ultimate liability for returned items and that the bank is attempting to protect them from further financial harm. The return of the item may cause valid payments to be declined for lack of funds or the client may release merchandise (selling a car, personal item etc.) based on the believe the item was paid.

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

We would not recommend supporting the softening of permissible customer communications under SAR confidentiality rules.

13. The Board, FDIC, and OCC have received complaints from supervised institutions regarding challenges in resolving disputes about liability for allegedly fraudulent checks. What is the experience of supervised institutions when trying to resolve these types of interbank disputes regarding allegedly fraudulent checks? Do these types of interbank disputes arise more frequently in connection with certain types of checks or parties? What actions could the Board, FDIC, and OCC consider, including potential amendments by the Board to Regulation CC, that could improve supervised institutions' ability to resolve interbank disputes over liability for allegedly fraudulent checks?

Altered item claims are regularly denied by the BOFD in conflict with the UCC Warranty policy/reclamation process. As a result, the BOFD rejects the claim as "non altered item", as known as, counterfeit without evidence. Upon further inquiry of the item and potential recoveries on behalf of the bank or the client, the BOFD will demand a "Hold harmless" agreement where one is not required. The result is extra work and time for both banks and a delay in the recovery of funds with a potential client impact.

Forged or missing endorsements are not, as a rule, reviewed by the BOFD in the industry. This is a known industry issue, as there are not technical services to support on a large scale, nor do the individual banks have capacity/funding to complete inspection manually. The result is an impact to the check issuer and a delayed discovery of an intercepted check that has been fraudulently endorsed.

Regulation CC does not apply to entity accounts. Enforcement of the duties under OCC Warranty claims and a systemic solution with a standard, detailed operating procedure on the sending and receiving of such claims with SOPs for administration of the program by all banks. There is a need to modernize regulations regarding check fraud - i.e., treasury regulations, Reg C, UCC, government agency regulations, banks' Terms & Conditions - all subject to varying levels of interpretation.

Yes, the ability for resolution on breach of warranty claims (altered and endorsement) has become difficult, many claims are taking more than 3 months to get a reply with resolution taking longer. The cause of the increase in volume is often contributed to increase in mail theft, the ability for an individual to assume a business identity due to the lack of state registration offices actively reviewing for fraud red flags and their not being required to follow FCRA identity theft red flags, which then allows a new account to be opened in the name of the original payee at a bank who relied on the state registration documents.

Many BOFD FIs are actively looking for denial reasons, vs. accepting responsibility that their client negotiated an item that wasn't valid. The BOFD by regulation is responsible for these items as they had not only the opportunity to review the original check at the time of negotiation and were in the best position to identify the alteration or endorsement issue, but they also completed the KYC of their client and are in the best position to recovery the funds should the repayment draw their account negative. Many BOFDs are attempting to deny items for invalid reasons, such as we require "proof" from the victim regarding the situation, need an updated affidavit or one that isn't applicable to the claim type these tactics delay resolution in what appears to be a desire to have the drawee bank drop the claim. Some banks are also counting on the fact that lower value claims won't be pursued in court. In essence these banks are ignoring their obligation to negotiate a valid item in an effort to reduce their fraud losses, while at the same time failing to properly address their KYC failures that continue to further allow these

issues. In some cases, the teams are not properly staffed or trained on the claim process causing unwarranted delays and harm to the drawee bank. Additionally, some banks require the claims by mail and fail to respond to questions regarding denials which can further unduly delay the resolution time.

To assist in resolving these situations the following should occur within the regulation:

A. The creation of a centralized avenue to submit and resolve claims, the process should include an arbitration process to allow the banks to discuss the matter to foster timely resolution.
B. The definition of an altered, forged maker should be further clarified to ensure consistent handling within the financial community. Checks that are validly issued and the payee or value changed and the maker's signature re-traced or added back to the check shouldn't be considered forged maker and absolving the bank of first deposit from their responsibility.
C. BOFDs who are unable to produce the original check should be obligated when there is a valid dispute regarding the authenticity of the check.
D. The establishment of a reasonable timeline for resolution or explanation to the drawee bank should be established and enforced by regulation.
E. Clearly articulate that the denial of an altered, endorsement claim and the bank of first deposit requiring a "hold harmless" should be prohibited. This tactic is use to delay payment of funds and the engagement of legal areas.
F. Review the current regulatory guidance and requirement landscape for check claims, modernize and address mis alignments. Consideration should also be given to having the UCC at a federal level vs. individual state adoption.
G. Modify the requirements for standard return reasons to ensure the maker bank is returning the item with enough information for the bank of first deposit to take action and mitigate the risk for the client and the bank. The most common example of this is checks returned within the 24-hour return window as "refer to maker".

The failure of the financial community to be able to resolve these items has caused a lack of faith amongst the banks and has impacted the consumer in a negative manner.

Although the Board is not proposing any changes to Regulation CC at this time, the Board seeks comment on the following questions:

14. Regulation CC seeks to balance prompt funds availability with the risk of checks being returned unpaid for reasons that include fraud. What potential amendments to Regulation CC would support timely access to funds from check deposits while providing depository institutions with sufficient time to identify suspected payments fraud?

While banks have invested heavily in technology to identify unusual check activity. It is difficult to often fully resolve the questionability of the item prior to the funds being required to be available under Regulation CC. Any reduction in the hold times currently within Regulation CC would negatively impact the client experience from a fraud perspective as well as be detrimental to the financial community. Many consumers are unwittingly a victim of fraud by receiving a payment that is later returned after they have released the funds or merchandise the check was

paying for. It would be beneficial to update the new account exception by removing the language within 229.13(a)(2) stating "An account is not considered a new account if each customer on the account has had, within 30 calendar days before the account is established, another account at the depositary bank for at least 30 calendar days", this would allow banks to properly address the risk of a new account based on their experience with the client and to consider the change that is taking place and the risk. Furthermore, criminals have no issue waiting 30 days for an account to become available for their fraudulent acts, it would be beneficial to extend the time frame to 60 or 90 days and remove the exception related to Treasury, Bank checks and allow banks to place holds at their discretion as criminals know the bank is required to release funds. Additionally, consideration should be made to reduce the "large deposit" hold values. Currently criminals are aware that they have the opportunity to obtain over $6,000.00 based on this exception. The reduction of this will discourage criminals and reduce funds being utilized for criminal acts.

The hold reason "reasonable cause to doubt collectability" should be further defined to allow full understanding of when this exception can be used.

Consideration should also be given to:

Allowing a FI to place a hold on incoming electronic payments where there is a reasonable belief that fraud is being perpetrated. As consumers follow the campaigns to cut back on checks criminals will return to the digital channel and the regulatory landscape must be equipped with the tools the banks need to stay a step ahead of the criminal.

Building in language that further clarifies the time that a bank can hold a payment directive from a client when suspected that it is the result of a scam.

What is acceptable for the volume of client outreach to address suspicious activity as well as the length of time to leave an account restriction in place to attempt to reduce the fraud impact to the client or bank. It should be noted that investigations are often complex, and the bank is dependent on communication from other stakeholders for information to make an educated determination of what has caused the activity to appear suspicious.

a) Have technological advancements in check processing reduced the time it takes for depository institutions to learn of nonpayment or fraud such that funds availability requirements for local checks and nonproprietary ATMs should be shortened?

No, the advancements in check clearing haven't advanced to the level of the check return being known prior to funds availability. The criminal enterprises understand the time it takes for items to be returned and know they have the ability to access the criminal profits from their actions prior to the check being returned. Additionally, the breach of warranty (altered and endorsement) process continues to be very manual in nature and handled differently by each bank. It would be beneficial for there to be a universal process with required timelines for resolution.

b) What effects would shortening funds availability requirements have on payments fraud, consumers who rely on timely access to funds, and depository institutions?

The shortening of funds availability will have a detrimental impact on the consumer and the banks, with the fraud losses to both being expected to rise significantly. While the availability of

"good" funds would be received faster we wouldn't have the ability to truly vet the authenticity of the payment prior to release and therefore raise the overall risk for the customer and bank.

Consumers today rely on the bank to "know" if the check is bad. The typical consumer believes that if the funds are available there is nothing wrong with the check. This is fundamentally wrong, as the check can be returned after the funds became available through the standard return process or through a breach of warranty claim. The reduction of funds availability holds will ultimately hurt the consumers who are least in a position to absorb that loss causing further distrust of the financial services community. Which in turn will further increase the unbanked community as they either have their account force closed due to a negative balance, or they close their accounts out of frustration and fear of the situation occurring again.

It should also be noted that the Treasury's current ability to return checks well outside of the Reg CC requirements is well known to criminals. The criminal takes advantage of this and will use the same account to negotiate multiple checks, relying on the fact that the Treasury won't return the item quickly. The current standard for return time frame from the Treasury should be reviewed and enhanced to more timely return the items to better align with the funds availability requirements.

c) Are there any changes the Board should consider to the expeditious return requirement to better balance providing expeditious notice to the receiving depository institution with ensuring adequate time for the paying depository institution to investigate potentially fraudulent checks?

There should be more open communication between the Fis in the event that a check is unable to be returned due to the expeditious return requirement, but the BOFD is unaware of the validity of the check. Also, endorsement issues (i.e., Forged endorsement claims) do not follow the same timelines and can return months later.

Regulation CC's objective of balancing prompt funds availability with mitigating check fraud risk remains important given ongoing fraud trends.

Technological advances have certainly made check processing faster and improved fraud detection, but these tools are not yet consistently available across all institutions.

While quicker funds availability benefits consumers, shortening timelines could unintentionally increase fraud losses, especially for smaller banks that don't have the same scale of resources. A more balanced approach may be to focus on improving fraud information-sharing and refining return notifications, so that institutions of all sizes can act quickly on suspected fraud while still supporting timely access to funds for consumers

Rather than shortening funds availability requirements at this time, the Board may wish to prioritize (i) industry adoption of standardized fraud data elements in check processing, (ii) improvements in fraud information-sharing frameworks, and (iii) incremental refinements to return requirements that increase the usefulness of fraud-related notifications. These steps would better balance consumer access with systemic risk management than across-the-board changes to availability timelines.

15. Regulation CC provides six exceptions that allow depository institutions to extend deposit hold periods for certain types of deposits, including deposits for which the

depository institution has reasonable cause to doubt the collectability of a check. Is this exception effective in allowing depository institutions to mitigate check fraud while also allowing timely access to funds? Would depository institutions benefit from further clarification on when it may be appropriate to invoke this exception? What are the experiences of businesses and consumers when depository institutions invoke this exception in order to delay the availability of depositors' funds?

Leveraging Fraud Technology Signals as a Basis for Holds

1. Advancements in fraud detection technology, including real-time image analysis, machine learning models, and behavioral analytics, now allow financial institutions to identify high-risk deposits within seconds of presentation. These tools can generate alerts based on signals such as:

A. Image forensics identifying altered or counterfeit checks

B. Data inconsistencies between the MICR line, payee name, and check amount

C. Account- and customer-level risk indicators (e.g., prior fraud history, unusual deposit patterns)

D. Cross-institution negative file matches or watchlists

We recommend that the Agencies explicitly acknowledge in Regulation CC guidance that such technology-generated fraud alerts may form part of a bank's "reasonable cause" to doubt collectability. This would empower institutions to act swiftly and consistently when fraud signals are present, reducing loss exposure and protecting consumers from downstream harm.

2. Clarifying the "Reasonable Cause" Standard

While the regulation references "reasonable cause," it does not provide a detailed operational definition or examples beyond traditional indicators (e.g., postdated checks, missing endorsements). This lack of clarity can lead to uncertainty and inconsistent application across institutions, particularly when relying on modern fraud detection methods that were not contemplated when the rule was originally written.

We recommend that the Agencies provide supplemental guidance to:

A. Define "reasonable cause" in a way that explicitly includes credible fraud risk indicators identified through automated or manual review.

B. Offer illustrative examples of fraud signals—both traditional and technology-driven—that may justify an extended hold.

C. Emphasize that institutions should document the specific fraud indicators supporting the hold decision to ensure compliance and transparency.

3. Balancing Fraud Prevention and Funds Availability

While extended holds are critical for preventing fraud losses, we recognize the importance of timely funds availability for legitimate customers. We encourage guidance that:

A. Urges institutions to apply the exception in a risk-based manner, using fraud alert severity and confidence scoring to determine hold length.

B. Recommends prompt release of funds if subsequent verification clears the fraud concern before the end of the hold period.

C. Encourages proactive customer communication, explaining the reason for the hold in clear, non-technical language.

4. Industry Experience

Our industry experience suggests that in cases where modern fraud detection alerts indicate high risk, holds applied under the "reasonable cause" exception have prevented significant fraud losses. However, absent clear regulatory acknowledgement that such alerts can support "reasonable cause," institutions may be hesitant to act, increasing exposure to losses and liability.

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

A requirement should be made to share non-card fraud payment data across the industry. It should be separated by retail/consumer and commercial with an ability to cross over segments for best practices development. Industry benchmarking - especially for entity/commercial accounts - is needed.

There is a lack of consortium groups focused on non-card fraud in the commercial space. This gap is significant because the onboarding process and overall behavior of commercial clients differ materially from retail clients, requiring distinct fraud solutions and tailored client management approaches.

There is a need for near real time fraud information sharing and red flags. This timeliness issue impacts the ability of a bank to detect and prevent fraud within its own walls and across FIs. This would aid in 'breaking the chain' of fraudulent money movement. Shared data should consist of transactional data (i.e. account level data) as well as other relevant identifiers (i.e. device IDs, IPs, bad bene info, etc.). Such information should be utilized to feed standard fraud detection services and systems used for real time and near real time decisioning (much done in batch today).

Information sharing can be improved by addressing the overarching fear of legal or regulatory reprimands for sharing client data. Many financial institutions view the sharing of any data related to fraud isn't allowable under the current 314A or 314B regulations or as a privacy concern as some legal teams say there is nothing that prohibits it, but nothing allows it therefore we will take the conservative approach and not share. All overlapping regulations must be clarified to clearly articulate that fraud is a permissible purpose, and the regulations must have adequate safe harbor clauses when done in an effort to stop fraud or scams or to create a case for law enforcement. Additionally, there must be encouragement for the bank to reply timely to the request as fraud is a in-progress act where delays may cost consumers their life savings.

The coordinated collection of fraud data with access to the FIs will enable the FI to reduce the risk to the client and to the bank of fraud occurring. The creation of a centralized fraud data base would also further create a tool for FIs to access to assist in the identification of accounts

or individuals actively involved in fraud or scams. Additionally, requiring banks to access a database that would confirm the account ownership of an account receiving a wire or other electronic payments would provide the FIs with a tool to reduce client risk of sending funds to an account that doesn't align to their electronic instructions. This process has been successful in the UK and would assist the bank when customer-facing staff are attempting to help the client realize they have been targeted as part of a scam. Additionally, a regulation that requires banks to review incoming electronic payments to match the intended recipient's name to their account that receives the credit. When the intended name and account name don't match there needs to be regulatory authority for the bank to hold the funds until an investigation can determine if the transaction is appropriate.

It would also be recommended to organize a working group of banks to determine the best way to support each other in fraud in progress requests to ensure they receive the priority needed to reduce fraud while also not creating undue hardship on those that rely on the banking system. Additionally, a universal way for a bank to inquire on the validity and funds availability of a check. This could be done through automated process or by having resources available to support the peer banks. It would be beneficial to build a process for fraud professionals to be able to authenticate other banks fraud professionals through a type of mutual authentication.

17. What barriers limit the collection and sharing of payments fraud data between industry stakeholders, and how could these barriers be alleviated? For example, have specific barriers limited development of solutions or participation in bilaterial or multilateral payments fraud data collection and information sharing? What changes would address these barriers?

Legal and Compliance uncertainty around data sharing and different interpretations of how to react to the data when received inhibits effective sharing and response. Industry antiquated systems and the ability to easily collect data in a standardized format, and delivery means (i.e. secure portals or direct feeds do not exist) limits sharing capabilities.

Much like card fraud, the ability to tag fraud transactions and carry the related detailed data (transactional and environment) into a system (i.e. MC SAFE, Visa RISK) does not exist for payment fraud (check, wire, ACH, RTP, etc.). Development of the standard AND a way to deliver the standardized details would be needed.

314b of the Patriot Act permits information sharing but there are no provisions that provide a Safe Harbor that would protect the bank which is sharing the information. Clearer Safe Harbor language would promote more effective info sharing.

The primary barrier for the collection of data to be used in fraud prevention purposes has been the overarching fear of regulatory reprimand as well as the legal consequences of providing data to a peer bank. As stated above, the clarification of regulatory requirements around the sharing of data related to a fraud situation and the inclusion of safe harbor for the bank when they have shared data in good faith to stop fraud and scam activity from entering the financial system is needed to address these barriers.

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

The agencies should help with the standardization of a fraud enterprise model and operational admin across payment types. Management of fraud is siloed by payment types (check, wire, ACH, RTP, etc.). Standardized typology guidance should be supported, but there is inconsistent adoption with different interpretations taken on by banks, and this results in poor data quality. The recommendation is that the FRS should continue to refine and promote the framework with specific administrative policies on the execution/processes with practical implementation guidance provided.

The sharing of data can provide valuable intelligence to the bank to further assist in the identification of scams or fraudulent activity. Frauds and scams continue to evolve at a fast pace and are often multi layered and complex. Today, fraud involves many data points to drive the investigation to the proper outcome. While there is no one list of data elements that solves all, it we recommend that the data shared involve the account ownership, length of account, status of the account, and channel of payment. In the fraud space the sharing of data around current fraud trends, those involved in the fraud scams with the account data would further allow banks to be proactive vs. reactive through a recovery investigation process. In consideration of the fraud and scam classifier the collection of fraud data while beneficial banks often have their own internal definitions and reporting restrictions based on resources, technology etc. If the goal is to know the true impact of fraud, a set standard needs to be created and required to properly document the impact of fraud and scams on the US financial system.

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

The types of fraud data that would have the largest impact on addressing payments fraud are those that provide granular, standardized, and comparable information across instruments, including both credits (incoming payments) and debits (outgoing payments). This would allow analysis at the transaction, account, and broader ecosystem level.

Key data include:

A. **Checks:** Payee and payor/beneficiary name, stock and signature interrogation data, and account status at the Bank of First Deposit (BOFD).

B. **Electronic payments (ACH, wire, RTP):** Payee and payor/beneficiary name, account status at BOFD, account type (consumer or commercial), static device-level data (e.g., IP address, device ID, known bad beneficiary lists), dynamic digital behavioral data, and standardized beneficiary naming conventions within transaction channels (avoiding free-text fields).

C. **Comparative transaction data:** Information on both credits and debits to enable detection of suspicious mismatches or circular flows at the transaction-, account-, and network-levels.

The most impactful fraud data for mitigating payments fraud would include:

A. **Granular transaction-level data** including payment channel, type, and timing to enable detection of anomalous patterns.

B. **Fraud typologies**, particularly around schemes such as account takeover, business email compromise, synthetic identity fraud, check fraud, and authorized push payment fraud.

C. **Loss and recovery outcomes**, to better understand systemic vulnerabilities and liability allocation.

D. **Cross-institutional linkages**, such as the identification of mule accounts or repeat offenders across multiple financial institutions.

Currently every institution reports fraud differently, which makes it hard to connect the dots across the industry. Standardized fraud reporting and a common taxonomy would make trend analysis and collective defense much stronger.

Banks and payment operators can collect this data, but it's regulators and agencies like FinCEN, the FBI IC3, or FS-ISAC that are best positioned to aggregate and share anonymized insights back with the industry in a secure way. A centralized fraud utility, or at least a federated sharing model, would materially improve prevention efforts and strengthen system-wide resilience.

In addition to what is stated above for data collection to help in the prevention of fraud and scams, a key aspect will be how the data can be accessed, filtered and utilized. The utilization of a centralized unit to fully track the fraud and scam losses occurring within the US would be beneficial. The tracking could include geographical areas as well as scam type to help further target direct education to consumers. The collection of true value that shows the consumer loss, the bank loss with the demographics of those targeted would provide significant value from a prevention and awareness perspective.

20. Is there a need for centralized databases or repositories for the sharing of payments 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?

Yes, however, it would be necessary to ensure security of access to such systems to avoid data breaches, maintain data integrity, and prevent potential corruption of said data

There must be clearly defined responsibility and liabilities by all banks - broken down by issuing bank, vs BOFD etc.

Cross agency collaboration would need to be required with the support of cross-industry efforts (social media, telecoms, etc.) to work with banking institutions, as fraud often commences first outside of the banking/ transactional walls. Identification of mule accounts, fake social media used for data collection, scam proliferation, etc. would be necessary. Collaboration with FinTechs would also be needed in the stakeholder group to develop a practical and useful solution. FinTechs would have to specifically support banking regulations and should be held to similar regulatory standards as banks.

21. How can the Reserve Banks enhance their existing risk management tools and services, operations, rules, or procedures to better meet the needs of participating financial institutions in addressing payments fraud? For example, should the Reserve

Banks consider requiring fraud reporting for payment rails (as they already do for the FedNow® Service) or adopting any particular payments fraud standards?

Recommendations:

A. **Standardized Fraud Taxonomy:** Develop a common language for fraud types to improve SAR filings and trend analysis.
B. **GenAI Tools:** Use LLMs to detect emerging scams and generate real-time educational content for consumers and bankers.
C. **Beneficiary Risk Scoring:** Alert institutions if a beneficiary has a fraud history. And an easy way for banks to report this information is to keep the data fresh and current.
D. **Trend Reporting:** Push fraud trends by region, age, and scam type to inform public and institutional responses.
E. **Free Screening Tools:** Provide accessible tools to help banks detect and prevent fraud like consortium data on beneficiary acct (name match, acct age, type of acct, etc.). New account opening and screening tools to prevent fraudulent accounts to be opened.

Yes, every additional reporting ask creates an additional burden on the FI taking away from prevention activities. The centralization of reporting to one agency would drive consistency and accuracy while allowing a holistic view of the overall impact of fraud and scams on the US consumer. The data should be considered highly classified with secure access restricted to appropriate personnel or agency. The security of the data would assist in obtaining compliance with this reporting objective. It's important to note that many consumers don't always report fraud to their bank. However, if the bank is doing reporting and the customer has reported to one of the multiple agencies currently available (consider consolidation of the agencies who accept reporting from consumers) the fraud numbers would be over reported. Additional context is provided in other questions.

The reserve operators have a network level view of the activity that is occurring. It would be beneficial for them to:

A. Take a more proactive approach of looking across the network to notify the banks of when items of suspicious nature have occurred. Sharing this information would allow the member banks to take a risk-based approach and potentially address an issue and stop future losses.
B. Require mandatory reporting when their channel is used for fraud allowing for a more comprehensive view of the fraud that occurs through their channel and allowing for enhancements to be based on the highest risk.
C. Require a validation process that enhances the FIs ability to ensure the intended recipient of the funds is who actually receives the credit at the receiving FI.

22. Are there risk management tools or services that the Reserve Banks should consider offering or expanding, such as a) developing a payments fraud contact directory for financial institutions, b) offering tools that can provide notification of atypical payment activity, or c) introducing confirmation of payee services to help mitigate fraudulent payment origination?

There is strong support in the industry for new tools and services:

A. **Fraud Contact Directory:** A centralized, secure directory for interbank communication that includes contacts for any payment method, updated, and current information.
B. **Atypical Activity Alerts:** Tools to flag unusual payment behavior in real time.
C. **Confirmation of Payee:** Industry-wide implementation to prevent misdirected or fraudulent payments.
D. **Standardized Communication Protocols:** Mandate consistent fraud investigation timelines and language across institutions, and a secure hub to communicate across payment channels and banks.

Why It Matters: These tools would significantly reduce business email compromise (BEC) and other high-impact frauds, while improving transparency and collaboration across the financial ecosystem.

A standard tool that works with the antiquated payment processing rails across banks in real time or near real-time information sharing to help mitigate payment fraud across all channels.

It would be beneficial to have the reserve or similar monitor the return of payments for detailed return reasons. The use of 'refer to maker' or other generic return reasons that may include fraud items is determinantal to the receiving bank and often allows fraud to go undetected and unreported.

It would be beneficial if all agencies involved in the transition of payments worked together to standardize the rules, return codes and timelines based on channel to allow for consistent treatment of the consumer and for ease of understanding and management by the financial services community. Regardless of the managing body i.e., NACHA, Federal Reserve, The Clearing House, EWS (Zelle) etc., consideration should be made to consolidate the rails to allow for a more efficient process and reduce overall cost and confusion to the consumer who often doesn't fully understand the difference especially in the digital payment arena.

NACHA should consider expanding the ability of RDFIs to return partial funds in cases of fraud or scam activity, regardless of how long the FI has had the funds. During the COVID pandemic many FIs fraud detection tools identified fraudulent credits. However, if even 1 cent was removed from the credit, they had no way to easily return the funds to the rightful owner most often the US Treasury but also state unemployment agencies. Banks have spent countless hours attempting to return funds back to the government. In some cases, banks are unable to get state level authorities respond to the request to return funds. In today's environment it is very time consuming to attempt to return partial funds especially to the US Treasury for ACH items that have sent to mule accounts not owned by the intended recipient - the implementation of a partial return window for ACH credits would be beneficial to all parties.

Additionally, while the ABA has put together a fraud directory open to all members and non-members including credit unions to assist with being able to locate people to assist with claim issues. Not all banks participate, the failure of banks to register causes additional operational burden on the drawee bank to attempt legal recoveries. It has been noticed that the smaller or internet banks are the ones who don't participate in the ABA Directory, and historically, they don't offer an easy way to reach a bank representative.

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?

A. CIB - Scams - Payment Diversions, Authorized Push Payments are most impactful to clients.
B. Second would be check fraud (all typologies).
C. A low volume (# of events) but high impact fraud type would be Account Takeover.

Numerous consumers are falling victim to organized scams. These scams include romance scams that turn into scams requesting payment or sharing of an investment opportunity that is false, unsolicited communication scams where the target receives a call, email or text from someone reporting to be from their bank, law enforcement, government agency, or a family member in need. Often these unsolicited communication/impersonation scams originate with a call and a spoofed number to the consumer. Victims of these scams can lose their life saving as well as their trust within the financial services community and in some case the emotional impact of falling prey to these criminals has caused emotional distress leading to death. Additionally, there is a societal impact of how the proceeds from these scams are used for downstream nefarious activities, drugs, guns, human trafficking etc. It is important to note the tactics used by the criminal can involve weeks to months of social engineering, the use of untraceable communication methods, the creation of AI sites, voices, photos and one of the most common is the ability to spoof calls, texts, and email headers. Criminals are not only going after electronic funds, but gift cards, cash, precious metals, etc. In some cases, they are leveraging Uber drivers for package pickup of non-electronic funds payments.

24. What measures, including technological solutions or services, have been most effective in identifying, preventing, and mitigating payments fraud at your institution? Are there actions that consumers can take that help institutions? For example, do financial institutions find it helpful when consumers alert the institution in advance when making large purchases, transferring large amounts of money, and traveling abroad?

A. Proactive Fraud Prevention Services (Payee Pos Pay, Reverse Pos Pay, Check Block, EPA debit block)
B. Client education
C. Strong authentication - all channels

25. To the extent not already addressed here, are there other actions that would support stakeholders in identifying, preventing, and mitigating payments fraud?

Standard intake process, identification of the type of payment fraud, and standard reporting.

A comprehensive review by banking and government officials to create statutory requirements around the definitions pertaining to the classification of fraud types (i.e., 1st party, 3rd party, synthetic, counterfeit etc.) and other common terms.

A review of the CRAPO Act with a lens towards allowing FIs to maintain copies of the identification used at the time of account opening in both the digital and in person channel. Current legislation has caused confusion on what data element scan be kept and used in what

circumstances. Additionally, concerns have been raised if the ID is maintained that can have an impact on those FIs that issue loans and downstream discrimination suits.

The creation of a working group of banking and government officials to document best practices to prevent fraud by channel (check, electronic, card etc.). This should be an exercise that would be updated periodically. This would assist both smaller FIs and larger FIs.

We would like to see industry collaboration with all stakeholders to evaluate how FIs can enhance their use of the digital footprint of a transaction to ensure the authenticity of a request.

A task force to ensure accountability of all stakeholders (telco, social media, fin tech, search engines, and vendors who have a role in the payment space) as it relates to regulatory compliance including identification of their client, the removal of bad actors, sharing of data to prevent the downstream impact from the bad actors. All parties need to be held accountability to ensure the overall digital and financial safety of the consumer eco-system.

The US Treasury should be asked to consider how they can strengthen their authentication process and validate that they are sending funds to an account that is owned by the intended payee. Additionally, NACHA should be encouraged to expand the usage of partial returns of fraudulent funds to allow the RDFI to return what they have available when they have reasonable knowledge of potential fraud.

The main bank trade organizations, such as ABA and BPI, have spent significant hours working to enhance the breach of warranty claim process. While progress has been made, the smaller banks who are not members of ABA or BPI continue to be slow and ineffective in their claim resolution. Additionally, they have created significant roadblocks for their peer banks to be able to contact them. We recommend that there be a group or communication channel created that reaches all FIs and Credit unions for faster claim resolution, faster fraud in progress resolution. All banks must have a fraud person on site during business hours to further enhance the industry's ability to address fraud in progress issues.

It is recommended that government agencies should clarify the ability of a bank to use age as a factor when developing fraud strategies. The inclusion of an older age would allow the banks to be more proactive to protect those who have historically have the most to lose and are often the most vulnerable to social engineering, manipulation and physical abuse. The use of a younger age may allow for anomalies behaviors to be identified timelier when the activity is outside of the expected for the account, i.e. college-age students who are targeted as mules, for the selling of their account. Collaboration on this allowance by the FI industry and the regulatory bodies will allow for effective implementation and proactive identification of suspicious activity.

26. Are there specific actions that commenters believe could encourage the use of payment methods with strong security features?

We would recommend that the use of digital payments be encouraged, and that there be a concentrated move away from historical means (e.g. checks).

The US government needs to support the movement from paper checks to electronic payment. The creation of a path to being paperless by 20xx.

Additional Comments:

A. Regulatory clarification/addendum to allow sharing of bad actor information between participants (resolve privacy challenges).

B. A bad actor list, like the OFAC Sanctions list, or incorporate a bad actor list into OFAC Sanctions list.

C. Centralized participant database for participants to publish and share fraud trends.

D. Greater deterrents and enforcement by law-enforcement agencies (prevention) rather than push responsibility to banks to stop on a transactional basis (cure).

E. Create a shared service to investigate and mitigate fraudulent activity, because a single fraudster does not only attack one bank.

F. Account Name vs Account Number checks will help reduce fraud, but contravenes UCC4a.

BAFT's comments reference the paragraph numbers in the consultation. BAFT looks forward to further dialogue on these important issues. For further information, please contact Deepa Sinha, SVP Payments and Financial Crimes, at [redacted]

Sincerely,

[redacted]

Deepa Sinha
SVP, Payments & Financial Crimes
BAFT
www.baft.org