BANK POLICY INSTITUTE

September 18, 2025

Via Electronic Mail

Department of Treasury, Office of the Comptroller of the Currency (OCC)
Board of Governors of the Federal Reserve System (Board)
Federal Deposit Insurance Corporation (FDIC)

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)*

To Whom It May Concern,

The Bank Policy Institute[1] appreciates the opportunity to respond to the *Request for Information on Potential Actions to Address Payments Fraud* (the RFI).[2] Fraud risk management is an important priority for all financial services providers and a concern for their customers. The Bank Policy Institute, through its technology policy division BITS, has been working with banks and government stakeholders for nearly three decades to help combat fraud. Examples of BPI-led initiatives include hosting executive forums to discuss fraud trends and threats, sharing effective practices for combatting fraud, partnering with the Financial Services Information Sharing and Analysis Center (FS-ISAC) and National Cyber Forensics and Training Alliance (NCFTA) to enhance fraud intelligence services, and engaging directly with other industries to enhance protections.

The fraud threat landscape has shifted in recent years. According to the FBI's Internet Crime Complaint Center (IC3), Americans reported fraud losses exceeding $16 billion in 2024, more than double the losses reported just three years earlier.[3] Financial institutions and their customers are facing increasingly diverse threats, including check fraud, sophisticated impersonations, authorized payment scams, account takeovers, and synthetic identity fraud.

Banks continue to invest in advanced fraud prevention technologies, including machine learning and artificial intelligence, to detect and disrupt these attacks. Yet the same emerging technologies are being weaponized by criminals to automate phishing campaigns, spoof communications, generate deepfake audio and video, forge documents, and mimic identities to bypass verification. These factors combined with the widespread availability of stolen personal and financial data are further fueling scams, account takeovers, fake account creation, and identity theft.

---

[1] The Bank Policy Institute is a nonpartisan public policy, research and advocacy group that represents universal banks, regional banks, and the major foreign banks doing business in the United States. BPI produces academic research and analysis on regulatory and monetary policy topics, analyzes and comments on proposed regulations, and represents the financial services industry with respect to cybersecurity, fraud, and other information security issues.

[2] Office of the Comptroller of the Currency, Board of Governors of the Federal Reserve System; and Federal Deposit Insurance Corporation, Request for Information on Potential Actions to Address Payments Fraud Request for Information Related to the Executive Order, "Modernizing Payments To and From America's Bank, 90 FR 26293 (June 18, 2025).

[3] 2024 FBI Internet Crime Complaint Center, Internet Crime Report, Annual Reports - Internet Crime Complaint Center (IC3)

This rapidly changing environment demands flexible supervisory and policy frameworks that allow institutions to respond to real world threats as they evolve. Banks need the ability to deploy real-time, risk-based interventions; obtain and share data across industries; and adapt to new fraud typologies without being constrained by outdated regulatory requirements or rigid compliance models. The regulatory framework should be updated to enable financial institutions to proactively protect consumers, focusing on the prevention of fraud schemes.

Executive Summary

Protecting consumers and the integrity of the payments system requires a fundamental shift: fraud cannot be treated as a bank-only problem. Fraud and scams are facilitated across various industries, agencies and platforms outside of banking. Thus, effectively addressing payments fraud requires cross-sector accountability, regulatory alignment, safe information sharing, and stronger operational controls to protect consumers, and preserve the trust and resilience of the U.S. payments system. A national strategy, led at the highest levels of government, must establish accountability across all sectors that enable scams. Telecommunications, technology, and social media companies must be required to implement robust anti-fraud programs with clear obligations and consequences for failure to act. Fintechs, which serve as key consumer-facing providers, must also be held to the same regulatory standards as banks to close dangerous gaps in oversight.

At the same time, outdated regulations limit banks' ability to intervene when fraud or scams are suspected. Modernization is essential to give financial institutions the flexibility to act in good faith to protect consumers without fear of supervisory or legal uncertainty. Agencies should authorize fraud holds on suspicious electronic payments, expand exception holds for potentially fraudulent checks, clarify definitions of "altered", "forged" and "washed" checks, and better align Treasury check processing timelines with fraud realities. Supervisory practices must also shift from process-based compliance to outcome-based oversight that supports proactive prevention and consumer protection.

Equally critical is the ability to share information across sectors in real time. Today, legal uncertainty discourages institutions from exchanging the very fraud data that could stop scams before funds leave the banking system. Congress and the agencies should establish safe harbors and guidance to enable cross-industry fraud information sharing, build standardized fraud and scam taxonomies, and reform SAR reporting to create actionable information exchange. Without these changes, institutions are forced to fight alone against adversaries who collaborate with speed and scale.

Finally, as the operator of critical payment rails, the Federal Reserve should embed fraud prevention capabilities directly into its systems—expanding fraud monitoring, standardizing reporting, and supporting Confirmation of Payee to protect consumers against authorized push payment scams. Treasury should also strengthen check verification processes with real-time tools that allow institutions to validate authenticity before funds are released.

Without decisive action, criminals will continue to exploit system gaps, leaving consumers and financial institutions to absorb the losses.

These recommendations are discussed in further detail below (formatted to follow the 5 sections of the RFI). BPI stands ready to work with the agencies to better address these complex issues and to develop a public-private plan to reduce fraud and scams and better protect consumers.

Understanding the Evolving Fraud Landscape

As the agencies consider actions after reviewing the RFI responses, it is critical to start with a shared understanding of how the fraud and scam landscape has fundamentally changed. Not all fraud is the same, and the strategies required to combat it vary significantly depending on the method, the victim's role in the transaction, and the enabling channels used by criminals. Without recognizing these differences, any policy response risks applying a one-size-fits-all approach that will fail to protect consumers and could even impede prevention efforts.

A clear distinction must be made between unauthorized fraud and authorized payment scams, as each demands different prevention strategies, operational responses, and regulatory considerations. Treating them as a single category would undermine effective policymaking.

- In the case of ***unauthorized* fraud**, the customer does not initiate the transaction. Controls such as login verification, device identification, AI-driven behavioral anomaly detection, and biometrics can be highly effective. In cases in which a bank suspects unauthorized fraud, banks can verify directly with their customers if they are in fact conducting the activity.
- For ***authorized payment scams***, criminals manipulate victims into authorizing transfers to accounts controlled by the criminals through romance scams, impersonation schemes, investment scams, or fake invoices. For the resulting payment, the real customer has initiated the payment, and the bank would not know whether or not the customer made that payment due to a scam. To help protect customers in these scenarios a bank would need to resort to subjective and subtle indicators to ascertain whether their customer was an unwitting victim of a scam. Even when bank staff alert customers they are likely the target of a scam, sometimes customers still insist on sending funds to the scammers. These attacks often unfold over days, weeks, or months with fraudsters building trust with the victim via email, phone, text, or social media.

In scam scenarios, authentication tools alone are ineffective because the customer is knowingly (but unwittingly) initiating the payment. Effective intervention requires detecting behavioral red flags, acting quickly, and persuading customers not to proceed, all while balancing consumer autonomy with the broader public interest in preventing scams. Banks have developed programs aimed at mitigating this challenge, but lasting progress requires flexibility, innovation, and shared accountability across industries whose platforms enable these crimes (social media, messaging, and telecommunications). Focusing only on whether a fraudulent payment occurred, without considering the entire life cycle of the crime – including how it occurred and who enabled it – would not be effective and would risk penalizing the institutions that are diligently working to stop it.

Section I: External Collaboration

Meaningfully addressing fraud and protecting the integrity of the U.S. payments system requires looking beyond the traditional banking sector. The current fraud environment, characterized by organized criminal networks, nation-state actors, insider threats, and cross-sector attacks, demands a coordinated national approach to address fraud at an earlier point in its life cycle.

Collaboration must extend to federal law enforcement, the U.S. Treasury, the Consumer Financial Protection Bureau ("CFPB"),[4] the FTC, the FCC, Department of Homeland Security ("DHS"), the Postal Inspection Service, and private-sector parties whose services and platforms are used to enable fraud, such as social media, telecommunications, and technology companies. These services and platforms are often

[4] The CFPB, in particular, has joint rulemaking authority with the Board for certain provisions of Regulation CC (Expedited Funds Availability) related to funds availability schedules, consumer disclosures, and exceptions allowing for extended holds to prevent check fraud.

the entry points for scams, yet they have fewer obligations than banks. Combating fraud and scams should be treated as a national priority, with federal leadership collaborating on comprehensive requirements and expectations across all relevant sectors that can combat malicious actors.

The following three recommendations outline initial steps to help close systemic gaps and strengthen prevention.

1.1: The Agencies should work with the FCC and the FTC to ensure all entities in the life-cycle of a scam or fraud event implement anti-fraud programs.

Telecommunications, social media, and technology firms must play a more direct role in helping to prevent fraud and scams facilitated on their platforms. These industries are now central vectors for fraud and scams, yet they lack the same sort of wholistic prevention and consumer protection measures required of banks. Section 230 of the Communications Decency Act has historically shielded these companies from liability for third-party content, which these entities have often cited as a reason for limited intervention.[5] While Section 230 does not bar proactive moderation, its broad protections have slowed the implementation of more consistent preventative controls that could prevent the initiation of many scams. By contrast, financial institutions are already subject to extensive requirements and obligations for fraud prevention and consumer protection, such as the Identity Theft Red Flags Rule under Fair Credit Reporting Act (FCRA)[6] and the Office of the Comptroller of Currency's (OCC) Fraud Risk Management guidance[7]. Ensuring that industries exploited by criminals to facilitate fraud implement proactive prevention and detection measures would close existing gaps and strengthen consumer protection.

Criminals are aggressively exploiting these regulatory gaps. On social media platforms, scammers frequently target victims using fake ads for investments or goods, fraudulent marketplace listings, and even recruitment of new scammers in public groups.[8] Communications and messaging services are routinely abused by criminals through the use of spoofed calls, text scams or "smishing",[9] and mass text campaigns

---

[5] Section 230 of the Communications Decency Act of 1996 ("CDA 230"), codified at 47 U.S.C. § 230(c)(1), provides that "[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." Courts have consistently interpreted this provision to grant broad immunity to online platforms from liability arising out of third-party content, including fraudulent or misleading posts, ads, or messages. See *Zeran v. America Online, Inc.*, 129 F.3d 327 (4th Cir. 1997) (holding AOL immune from liability for failing to remove defamatory messages posted by a third party); *Force v. Facebook, Inc.*, 934 F.3d 53 (2d Cir. 2019) (extending immunity to claims alleging that Facebook's platform was used to facilitate terrorist activity).

[6] 16 CFR 681.2 – Identity Theft Red Flags Rule, established under Section 114 of the Fair and Accurate Credit Transactions Act of 2003

[7] OCC Bulletin 2019-37, "Operational Risk: Fraud Risk Management Principles"

[8] According to a May 2025 Wall Street Journal Report, "Meta Platforms, the parent company of Facebook and Instagram, is increasingly a cornerstone of the internet fraud economy, according to regulators, banks and internal documents reviewed by The Wall Street Journal… British and Australian regulators have found similar levels of fraud originating on Meta's platforms. An internal analysis from 2022 described in company documents likewise found that 70% of newly active advertisers on the platform are promoting scams, illicit goods or "low quality" products… Current and former employees say Meta is reluctant to add impediments for ad-buying clients who drove a 22% increase in its advertising business last year to over $160 billion. Even after users demonstrate a history of scamming, Meta balks at removing them. One late 2024 document reviewed by the Journal shows that the company will allow advertisers to accrue between eight and 32 automated "strikes" for financial fraud before it bans their accounts." Meta Battles an 'Epidemic of Scams' as Criminals Flood Instagram and Facebook - WSJ

[9] Smishing, derived from "SMS" and "phishing," is a type of cybercrime that uses deceptive text messages to manipulate victims into divulging sensitive personal information such as bank account details, credit card numbers and login credentials.

powered by SIM farms.[10] These tactics create systemic vulnerabilities that financial institutions alone cannot fix.

Some platforms have begun experimenting with solutions—scam labeling, voluntary takedowns, or fraud warnings—but these efforts remain fragmented and insufficient. A more durable framework should focus on aligning incentives across sectors so that prevention becomes both an economic and compliance imperative.

Federal bank regulators, including the CFPB, working in partnership with the FCC and the FTC, should develop consistent obligations for telecom, technology, and social media companies to implement anti-fraud programs. These programs must focus on preventing criminals using these platforms to initiate scams or fraud which will reduce the number of fraud or scam payments. These obligations should include meaningful consequences for non-compliance and create incentives for innovation in scam detection, customer alerts, and cross-sector prevention.

For social media companies these measures might include:

- Implementing "Know Your Merchant" identity verification standards and verification of ad ownership and brand authorization before ads are published.
- Removing impersonated profiles, fraudulent ads, and scam marketplace listings promptly after identification.
- Providing consumer alerts when suspicious links or content are detected.
- Reporting confirmed scam activity to a national registry and law enforcement in a timely manner.
- Developing standardized, cross-platform consumer reporting mechanisms.
- Actively disrupting scam training and recruitment sites.
- Standardizing reporting and intelligence-sharing processes with financial institutions to protect shared customers.

In the case of telecommunications and messaging providers (including SMS, RCS, iMessage, and OTT services), measures might include:

- Authenticating all U.S. calls through the FCC mandated STIR/SHAKEN standard.[11]
- Alerting consumers to unauthenticated calls or messages, especially those originating internationally.
- Deploying robust international anti-scam filters to block spoofing and mass campaigns.
- Enforcing anti-fraud standards consistently across Mobile Virtual Network Operators (MVNOs).
- Sharing confirmed scam numbers and traffic data across carriers.
- Enabling consumers to report scam messages in addition to spam.
- Introducing scam alerts like those offered in Google Messages.
- Adopting stronger Know-Your-Customer controls to prevent criminals from using telecom accounts to disseminate scams.

[10]A SIM farm is a sophisticated setup that uses multiple SIM cards to send large volumes of messages quickly, often for fraudulent purposes. These farms exploit telecom networks to send bulk scam texts, phishing messages, or create large numbers of online accounts, significantly increasing the risk of scams and fraud. By automating the process, SIM farms allow scammers to target a vast number of people at a low cost, making it easier to perpetrate scams and compromise personal information.

[11] STIR/SHAKEN stands for Secure Telephone Identity Revisited (STIR) and Signature-based Handling of Asserted Information Using tokens (SHAKEN). This suite of protocols aims to reduce the prevalence of fraudulent robocalls and caller ID spoofing, which have become significant issues in telecommunications.

By setting consistent standards across sectors, regulators can ensure that prevention begins where scams originate, not just belatedly when funds are already in motion.

1.2: Establish a White House Led National Strategy to Combat Scams

To be most effective, the agencies should support a coordinated national framework led by the White House. Like the Administration's appointment of an AI and cryptocurrency czar, a federal lead for scam and fraud prevention could unify public and private efforts, align regulatory approaches, and drive proactive data-informed mitigation strategies. This is not only about protecting consumers, but also about safeguarding the resilience and soundness of the U.S. financial system against industrialized criminal activity.

As Fifth Third Bank CEO and BITS Executive Committee Chair Tim Spence noted in a recent op-ed, *"America is behind in the scam fight: Why this bank CEO wants a national strategy"*, the U.S. lacks a central office charged with coordinating efforts across industries and sectors.[12] Unlike the U.K., Singapore, or Australia, the U.S. has yet to establish a single point of leadership to drive accountability across enabling platforms, regulators, and law enforcement.

Recent congressional proposals such as the Scam Safe Act (S.2019)[13] and the Fraud and Scam Reduction Act (H.R. 4936)[14], underscore the urgent need for action. These bills would enhance coordination, data-sharing, and consumer protections, reflecting important steps forward. Yet, their focus remains within legislative and agency boundaries. A truly empowered White House leader, able to work across sectors and government silos, is necessary to ensure integration, accountability, and consistent prioritization.

A dedicated initiative by the White House could:

- Coordinate interagency fraud strategy and oversight.
- Lead partnerships with telecom, tech, and social media platforms.
- Direct law enforcement prioritization of scams.
- Engage diplomatically to press foreign governments on prosecuting cross-border fraud.
- Coordinate at the state level with relation to law enforcement and education programs.

This type of centralized leadership would help the U.S. transition from today's fragmented, reactive approach toward a proactive and unified national framework. This shift would not only better protect consumers but also strengthen the resilience, safety, and soundness of the broader U.S. financial system.

1.3: Hold Fintechs to the Same Regulatory Standards as Banks

Fintechs are now central to the payments ecosystem, yet many operate under lighter regulatory and supervisory regimes. Those licensed only as state money transmitters or partnering with banks often avoid direct federal oversight, creating regulatory arbitrage and gaps in consumer protection. These gaps leave consumers exposed to fraud and scams, which frequently flow through apps like Cash App, Venmo, or crypto accounts where controls are weaker due to less robust oversight.

BPI has previously called for regulatory parity between banks and fintechs through comment letters that stress fintechs must meet the same standards for fraud prevention, customer verification, cybersecurity, and disclosures as banks.[15] Fintech-bank partnerships should also face rigorous oversight consistent with

---

[12] Spence, T. (2025, April 1). *The federal government needs to lead the fight against scams and fraud. American Banker*.

[13] Text - S.2019 - 119th Congress (2025-2026): TRAPS Act | Congress.gov | Library of Congress

[14] TRAPS Act (H.R. 4936) - GovTrack.us

[15] See BPI Comment Letter, October, 30 2024; Regulators Should Take the Reins on Fintech Oversight - Bank Policy Institute

federal third-party risk management guidance. Regulation must be based on function and risk—not charter or business model.

Consumers generally assume banks and fintechs provide equivalent protections. When weaker rules apply to one segment, criminals exploit the gap consumers misdirect blame. Equal standards for all providers handling consumer funds are essential to protect consumers and preserve trust in the financial system.

Section II: Consumer, Business, and Industry Education

BPI agrees that education is a critical tool, alongside other prevention measures, to protect consumers and businesses from fraud. Banks already have undertaken extensive efforts aimed not only at raising awareness but also at helping customers recognize fraud and scam attempts in real time. Examples of education efforts deployed by banks include:

- In-app warnings during high-risk transactions, especially when sending funds to new recipients.
- Email, SMS, and social media alerts about trending fraud and scam activity.
- Staff training for call center and branch employees to spot customers under duress or being coached by scammers.
- Targeted campaigns addressing phishing, business email compromise (BEC), impersonation, and romance fraud.
- Partnerships with consumer groups, community organizations, and law enforcement to broaden outreach and prevention.

While these efforts are extensive, the federal government plays a vital role in unifying and amplifying fraud education: the government simply can reach more consumers than any individual bank. Coordinated cross-sector campaigns can ensure consistent messaging, greater reach, and targeted outreach to vulnerable groups. Education must also extend to businesses, nonbanks, and technology platforms that interact with payment systems or customer data.

2.1: The agencies should coordinate with industry and other government agencies to promote consistent and coordinated messaging campaigns

The agencies should explore how they can provide leadership in coordinating consistent education approaches. The agencies should lead in coordinating consistent national fraud education. This includes promoting clear messaging on common scams, launching public-private campaigns modeled on initiatives like “Smokey the Bear,” and ensuring inclusive outreach with tailored content for vulnerable groups through community networks and multilingual platforms. They should also support small business education, particularly for nonbank participants and smaller institutions with limited resources. Together, these actions would create a more cohesive and effective national strategy for fraud education and prevention.

Section III: Bank Regulation and Supervision

The current regulatory and supervisory framework must evolve to meet the realities of today’s rapidly changing fraud and scams landscape. Consumers and financial institutions face unprecedented threats, from large-scale check fraud schemes and account takeovers to scams that manipulate consumers into authorizing payments to criminals. Yet the regulatory tools and oversight environment have not kept pace, hampering efforts to quickly and effectively combat these crimes. Regulation and supervision must shift from rigid process enforcement to a more flexible approach that prioritizes fraud prevention as a core component of both consumer protection and safe and sound banking.

Banks are increasingly placed in a difficult position when balancing fraud prevention with regulatory and funds availability requirements. If they intervene to help prevent a suspected fraudulent transaction, by holding funds or restricting account access – they risk liability under Unfair, Deceptive, & Abusive Acts and Practices **(**UDAAP) or other regulations. If they do not, they risk being faulted for inadequate controls exposing themselves to fraud losses, or reputational harm. This conflicting environment ultimately undermines consumer protection. The regulatory framework must be modernized to give banks the flexibility to act decisively against evolving fraud threats without fear of punitive consequences for reasonable, risk-based measures.

In relation to the RFI questions on Bank Regulation and Supervision, BPI provides recommendations below focused on two areas: 1) Modernizing regulation and supervisory approaches aimed at protecting customers, and 2) Modernizing Regulation CC to better manage fraud and improve check processing.

Modernizing regulation and supervisory approaches aimed at protecting customers (3.1 - 3.2)

As fraud threats increase and faster payment options expand, financial institutions need updated regulatory flexibility to detect and pause suspicious transactions—both inbound and outbound—in real time. Banks currently have limited ability to temporarily hold suspicious electronic deposits to verify legitimacy, especially in scam scenarios, where manual review or confirmation with the originator may be necessary. Criminals will often move money from accounts as soon as those funds become available, making it critical that banks can hold these payments when a fraudulent transaction or scam is suspected. Given the complex nature of today's fraud and scams, these investigations can take time and banks need flexibility in applying the appropriate holds.

While some institutions have implemented fraud detection tools for incoming electronic payments, there is no clear regulatory authority to pause, review, or return suspicious funds before they are credited to an account and made available for withdrawal. In practice, account-level restrictions have become an essential tool for preventing additional losses once fraud is suspected. For example, when a receiving bank is notified that a payment was sent to a potentially fraudulent account, it must investigate whether the recipient is an innocent customer or a complicit money mule.[16] These investigations are complex, time-intensive, and subject to regulatory uncertainty. Conflicting guidance from examiners and concerns about UDAP/UDAAP liability risk discourage banks from applying holds—even when the intent is to protect consumers. A 2022 CFPB consent order illustrates this challenge, where a bank's fraud-prevention practices led to penalties despite being aimed at blocking fraudulent deposits.[17]

3.1: Create a framework for fraud holds for electronic payments and enable banks to effectively manage anti-fraud measures and funds availability.

Other applicable laws, such as the anti-money laundering provisions of the USA Patriot Act, should permit banks to place extended holds on electronic deposits based on suspected fraud without violating the next business day availability requirements of Regulation CC (12 C.F.R. § 229.10(b)). The Board, the CFPB, and the other Federal banking agencies should not construe the Expedited Funds Availability Act ("EFAA") and Regulation CC as operating in a vacuum but should acknowledge that expedited funds availability requirements must work in tandem with laws and regulations focused on fraud prevention, anti-money laundering, and counter-terrorist or other illicit financing. To address this, the agencies should explore the following actions:

---

[16] A money mule is someone who receives and moves money that came from victims of fraud. Some money mules know they are assisting with criminal activity, but others are unaware that their actions are helping fraudsters.

[17]Consumer Financial Protection Bureau. (2022, December 20). *Consent order: In the matter of Wells Fargo Bank, N.A.* (File No. 2022-CFPB-0011). U.S. Government.

Item-Level Holds for Electronic Deposits

- The Board should adopt a new comment to Section 229.10(b) of Regulation CC clarifying that, although the exceptions in Section 229.13 do not apply to electronic payments, other fraud-related and AML obligations may supersede the obligation to provide next-day availability.
- Alternatively, the Board and CFPB could amend the interpretation of when an electronic payment is received under the EFAA and Regulation CC to add a third prong under 12 C.F.R. § 229.10(b)(2) which defines when an electronic payment is received to include "and (iii) complied with the bank's policies on reasonable fraud screening processes." This third prong would allow banks to use fraud screening tools to detect potentially fraudulent transactions and investigate such transactions before making the funds available.[18]
- Reasonable fraud screening practices could include:
    - Use of prudent processes designed to identify transactions at risk of fraud or scams
    - Use of fraud-imaging or fraud-logic tools predictive of high return rates
    - Detection of anomalous activity through AI, machine learning, or behavioral models
    - Notification from the sending institution confirming suspected fraud or scam
    - Evidence of unauthorized account access
    - Evidence the customer is a suspected scam victim

Account-Level Restrictions

- The agencies and the CFPB should engage with industry to confirm that banks may impose temporary account restrictions to protect consumers, including expectations for communication, documentation, timeframes, and safe release of funds when there is reason to suspect fraud or scam.
- Guidance should leverage the criteria above for a broader "reasonable cause to suspect fraud or scam" standard, enabling banks to act decisively while minimizing disruption.
- Banks should have sufficient time for investigation, particularly in first-party fraud scenarios, before funds are withdrawn or dissipated.
- Institutions should have a safe harbor from regulatory action when holds or restrictions are applied in good faith to protect consumers.

Regulatory Authority to Block or Delay Payments Based on Risk

- Banks must be able to delay or block payments when scam indicators are present, even if the customer appears to authorize the transaction.
- The agencies should work with the CFPB, which has authority under both the EFAA and the Electronic Fund Transfer Act ("EFTA"), to propose regulations regarding disclosure of the terms and conditions of the consumer's account. Effective disclosure of potential fraud prevention restrictions, and how they may affect the availability of check, cash, and electronic payment deposits, provides transparency and can help reduce consumer complaints. Effective disclosures also help mitigate UDAP/UDAAP risk. For electronic payments (other than wire transfers), the EFTA and Regulation E permit financial institutions to include in their initial disclosures account-level restrictions on the amount and frequency of transfers. These disclosures could be construed to give financial institutions the ability to disclose that they may defer or delay the processing of EFTs for a reasonable period of time to allow for the application of effective fraud detection and fraud prevention measures when they have a reasonable suspicion of fraud or a scam.

[18] The new regulation would read payment is not received until the bank has (i) received "payment in actually and finally collected funds"; (ii) received "information on the account and amount to be credited"; and (iii) complied with the bank's policies on reasonable fraud screening processes.

- The agencies, along with the CFPB and FTC, also should make clear that a bank has ability to intervene and delay or block payments when scam indicators are detected, even if the customer appears to be authorizing the transaction, and not be vulnerable to violating UDAP or UDAAP or other laws for delaying or blocking payments. The agencies should work with the CFPB and FTC to ensure consistent UDAP/UDAAP guidance regarding permissible payment holds, delays, or blocks.

Additional Regulatory Clarity

- Banks would benefit from having a clearer direction on incorporating age-based fraud risk factors into prevention strategies without violating fair lending laws, particularly the Equal Credit Opportunity Act (ECOA) and Regulation B. Fraudsters disproportionately target elderly populations, and banks need safe, consistent parameters to incorporate this risk factor responsibly.

3.2: Focus Supervision on Effective Fraud Prevention

To effectively combat fraud and scam threats, the supervisory framework must shift from box-checking compliance to collaborative, outcomes-based oversight that prioritizes prevention and consumer protection. Today, exams too often focus on technical procedures or isolated control gaps rather than whether banks' actions are effective in reducing fraud. For instance, examiners may flag account restrictions without acknowledging that such measures were taken to prevent suspected fraud and protect consumers.

This narrow approach risks distorting supervisory objectives. Examinations should evaluate bank actions in context, weighing process issues against fraud-prevention outcomes. Compliance and safety-and-soundness oversight should both support effective prevention programs, aligned with each bank's documented fraud risk tolerance and ability to adapt to emerging threats.

A modernized model would also use exams to surface trends, encourage regulator-bank information sharing, and highlight systemic issues such as cross-platform scams and novel attack methods.

Ultimately, supervisory oversight should enforce accountability while also enabling banks to dedicate more capacity to the shared mission of protecting consumers and the integrity of the payments system.

Modernize Regulation CC to Better Manage Fraud and Improve Check Processing (3.3 - 3.5)

The regulatory framework for check deposits and collections is outdated, fragmented, and ill-equipped to address today's elevated fraud risks and modern payment technologies. Rules are dispersed across Regulation CC, the Uniform Commercial Code (UCC), electronic check image exchange network rules (ECCHO), Treasury regulations, agency guidance, and varying bank agreements. Further complicating this state of affairs is the fact that states have adopted different versions of the UCC, which is further subject to varying interpretation by different courts.[19]

Check fraud has surged in recent years, driven by mail-system vulnerabilities, widespread availability of check-washing tools, and criminals' focus on exploiting this antiquated payment method. Between March 2020 and February 2021, the U.S. Postal Inspection Service received over 299,000 mail theft complaints, a 161% year-over-year increase. From February to August 2023, FinCEN logged 15,417 mail-theft-related check fraud reports involving $688 million in losses. At the same time, stolen check data are openly sold on

[19] Further penalties arising out of such activities may also be grounded in Unfair Deceptive Abusive Acts and Practices (UDAAP) by financial institution regulators.

the dark-web[20] and social platforms such as Telegram[21], enabling organized criminal rings to conduct large-scale forgery, alteration, and counterfeit schemes.

The surge in check fraud has left banks with high volumes of claims and disputes, exposing the limits of outdated legal and operational processes, creating delays for customers and disproportionate burdens for smaller financial institutions lacking the resources to absorb rising losses or manage complex disputes.

Absent a wholesale restructuring of the check collections process (which regulators have acknowledged was based on the presumption that banks generally handle checks in paper form),[22] the regulatory framework for check collections and funds availability requires enhancement to provide clarity as to parties' rights and obligations, streamline interbank dispute resolution processes, and facilitate fraud risk management and prevention. Below we provide recommendations for modifications to the existing regulatory framework to help solve these critical challenges, while striking a balance between fraud risk management and expedited funds availability. In addition to the below recommendations, we encourage discussions between the agencies and financial institutions on a roadmap to reduce and eventually eliminate paper check usage.

3.3: Allow banks to place exception holds on check deposits specifically when a fraud or scam is suspected

The current exceptions defined in Regulation CC, including the "reasonable cause to doubt collectability" provision, are not sufficient tools for mitigating check fraud. As currently framed, the Board's guidance for circumstances in which the exception may be invoked primarily pertain to the likelihood that funds are available in the drawer's account. This guidance does not clearly provide that fraud-related anomalies, such as sudden changes in the deposit customer's behavior or high-risk deposit patterns, can be considered when placing a hold under this exception.[23] Furthermore, "reasonableness" standards are largely open to interpretation, further complicating compliance and exposing supervised institutions and consumers to risk.

To effectively combat fraud, banks should have the flexibility to place holds based on the deposit bank's own fraud detection systems, evolving fraud trends, and other risk-based indicators. Fraud prevention controls vary depending on available technology, internal operations, and criminal tactics, and banks must be able to apply deposit holds using a holistic assessment of risk, not just availability of funds or account tenure, which alone are insufficient indicators of fraud.

BPI recommends the Board and CFPB revise the "reasonable cause to doubt collectability" exception to encompass situations where a bank has a good-faith belief that an item is unusual or suspicious and may be the result of fraud. Alternatively, the Agencies could recommend that Congress amend the EFAA (12 U.S.C.

---

[20] Reports suggest that listings on the dark web for "check bundles" range in price from $1,000 to $100,000. *Mail Theft, Dark Web Sales, and Counterfeits: Combating Today's Check Fraud Threats*, SQN BANKING SYSTEMS

[21] NBC4 Washington. (2023, February 14). *Criminals use Telegram to recruit 'walkers' as America's big banks see an 84% increase in check fraud*. NBC4 Washington.

[22] 76 Fed. Reg. 16862, 16862 ("Subpart C's provisions presume that banks generally handle checks in paper form. Since the provisions were adopted in 1988, however, banks have largely migrated to an electronic interbank check collection and return system.").

[23] The Board's current guidance identifies the following examples of circumstances under which this exception may be invoked, each of which pertain to the likelihood that funds are available in the drawer's account: (i) information received from the paying bank regarding the actual or likely nonpayment on a check (e.g., due to insufficient funds, stop payment order); (ii) stale or post-dated checks; (iii) reasonable belief that the depositor is engaging in kiting activity; and/or (iv) reasonable belief as to the insolvency or pending insolvency of the drawer of the check or the drawee bank. 12 CFR part 229, App. E, § F.229.13(e)-2

§ 4003) to establish a *new exception* allowing for holds on checks in circumstances where fraud or scam is suspected.

As an alternative to the existing reasonableness standard, the revised (or new) exception should make clear, in regulation or commentary, the basis upon which it can be invoked when a bank has a good faith belief of "unusual" or "suspicious" (likely fraudulent) activity based on a customer's risk profile and indicators such as:

- Use of reasonable and prudent processes and procedures to identify transactions at risk of fraud or scam.
- Reliance on fraud imaging analysis tools or fraud logic rules validated to predict high rates of returns.
- Detection of unusual or anomalous activity through machine learning, AI, or other anomaly-detection models.
- Evidence suggesting a customer is a victim of a scam or other fraud.[24]

Updating the exception framework in this way would give banks the necessary flexibility to apply risk-based holds in good faith, enabling earlier intervention against fraud while preserving consumer protection and maintaining confidence in the safety and soundness of the payments system.

3.4: Revise the definition and exception for "new accounts" to better align with risk trends

If updated, the "new accounts" exception is another that could be very helpful to institutions as a fraud prevention measure, as many fraud cases arise in the early life of an account. The exception narrowly defines a new account to an account opened in the last 30 days. Fraudsters exploit this by opening accounts, letting them "age," and conducting small-dollar transactions to build a veneer of legitimacy before committing large-scale fraud.

The rule also fails to provide hold authority for new accounts added to an existing relationship. Criminals are aware of this loophole and often open additional accounts to avoid new account holds altogether. This practice makes it difficult for banks to intervene, even when fraud risk is high.

Expanding the scope of the new account exception, through statutory or regulatory changes, would strengthen banks' ability to apply risk-based holds to suspicious accounts, verify authenticity of customers, and detect unauthorized or fraudulent activity before losses escalate. Therefore, we recommend consideration of the following actions:

- The Board and the CFPB should close the loophole for customers that hold another account with the depository bank and allow for an account to be treated as a "new account" whenever there is a change in authorized signers or account titling.[25]
- The time period during which an account is deemed a "new account" should be amended from 30 days to 120 days. This would allow institutions to establish an understanding of account/transaction behavior and afford customers appropriate time to report unauthorized activity, considering standard monthly bank statement cycles.[26]
- All check deposits should qualify for the "new accounts" exception and eliminate the special rules for greater next-day or second-day funds availability for certain types of check deposits (including

[24] These criteria should be used to replace the existing reasonableness standard as it relates to fraud related holds.

[25] This could be done by eliminating the language within Regulation CC, 12 C.F.R. § 229.13(a)(2) stating that "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".

[26] This change would likely require that Congress amend the EFAA (12 U.S.C. § 4002(a)).

certain Treasury checks, USPS money orders, state or local government checks, and cashier's, certified, or teller's checks) but maintain the requirement for next-day or second-day availability up to the first $6,725 of funds deposited on any given banking day.[27]

3.5: Revise Regulation CC's "Presumption of Alteration" provision and Clarify Key Terms

The surge in sophisticated check fraud, combined with widespread use of truncation and image exchange, has exacerbated confusion over how to classify and resolve fraudulent items. Banks face persistent disputes over funds availability, return obligations, fraud type determinations, and liability allocations. A central challenge is the lack of clarity and consistency in defining fraudulent checks. The distinction between "forged maker," "altered," and "counterfeit" checks has grown increasingly blurred as modern methods—such as chemical "check washing" and digital alterations—combine elements of forgery and alteration.

The existing framework under Regulation CC and the UCC, developed in an era of paper processing, fails to address these typologies. Courts have struggled to apply outdated definitions, producing inconsistent rulings that often hinge on technicalities. These gaps prolong interbank disputes, drive up costs, and ultimately delay access to funds for consumers.

Check "washing" illustrates the problem. Some banks and courts treat a completely washed check, which includes washing of the signature, as a forged maker's signature, assigning liability to the paying bank. Others classify it as an alteration, shifting responsibility under presentment and transfer warranties to the bank of first deposit.[28] Disputes intensify when the fraudster substitutes a signature with a different name, further complicating the classification.

The Board's 2018 "Presumption of Alteration" was intended to clarify who should hold the loss when only an image of the original paper check is able to be produced as evidence given the split decisions in the courts at the time and to simplify these disputes but has, in practice, created additional ambiguity.[29] When the original paper check is no longer able to be produced as evidence in a check dispute, the rule provides and evidentiary presumption that check was altered unless proven otherwise.[30] Yet the ability to rebut the presumption depends on producing either the original paper check, i.e., the "original check," which is rarely available in today's environment, as the vast majority of checks are cleared via electronic check image exchange. Only the bank of first deposit has the ability to require its own customers deposit the physical original paper checks rather than use of remote deposit capture. Paying banks can no longer demand presentment of the original paper check before being liable on the item. Other forms of rebuttable evidence can be used, including other images of validly issued checks for comparison of the check stock features which survive truncation. The reliance on a "preponderance of evidence" standard often leads to costly expert testimony, undermining efficiency and encouraging litigation.[31]

---

[27] This change would likely require that Congress amend the EFAA (12 U.S.C. § 4002(a)(1) and 12 U.S.C. § 4003(a)(3)).

[28] *Fidelity Brokerage Services LLC v. Pacific Western Bank*, No. 2:23-cv-09760-RGK-MRW, 2024 WL 4874558 (C.D. Cal. Sept. 20, 2024) (distinguishing between checks that were never validly issued and those that were validly issued but subsequently modified to reflect an intention contrary to that of the drawee); *see also Provident Savings Bank, F.S.B. v. Focus Bank*, 548 F. Supp. 3d 862 (E.D. Mo. 2021) (finding that a digitally altered copy of a check which is unauthorized, modified and printed on new check paper is not an alteration under the UCC, and *Provident* clarified that a "washed" or altered check is not a forged maker check, reinforcing the UCC's distinction between alteration liability and forgery liability, which continues to influence check fraud disputes today).

[29] 12 CFR § 229.38(i)(1)-(3).

[30] 12 CFR § 229.38(i)(1)-(2).

[31] *Id.*

Given the prevalence of check washing and evolving fraud methods, the Board should reassess whether the presumption is serving its intended purpose. Specifically, it should (i) define "original check" more precisely, (ii) clarify distinctions between altered and forged items, and (iii) issue guidance on satisfying evidentiary standards without reliance on paper checks or expert testimony.

While broader changes to the UCC require lengthy processes across multiple jurisdictions, the Board—working with other agencies—is well positioned to lead a targeted initiative. A working group of banks, trade associations, and other stakeholders should be convened to examine current typologies, develop updated definitions, and establish liability rules that reflect which institution is best placed to prevent losses given modern processing and technology. Harmonizing definitions across Regulation CC and the UCC would promote clarity, streamline dispute resolution, and strengthen the fraud-prevention ecosystem.

While the Uniform Law Commission plays a central role in this context, the UCC rulemaking process is long and cumbersome, requiring adoption by every state, and still open to varying interpretations. BPI recommends that the Board, in coordination with the other agencies, establish a small and targeted working group of banks, trade organizations, and other key stakeholders in an effort to: (i) examine current check fraud typologies and trends; (ii) develop definitions to delineate and clarify different types of fraud and, in particular, define check "washing" in a manner that makes clear whether such fraud constitutes an alteration or a forgery; and (iii) clarify the economically sensible allocation of liability for washed checks, taking into consideration which bank is best able to prevent fraud losses at the lowest cost in light of contemporary check processing methods. While changes in fraud-related definitions ideally should be made in, and harmonized across, Regulation CC and the UCC, BPI believes that the Board is uniquely positioned to spearhead this effort given its expertise in check processing and the regulation of check payments.

A revised definitional and liability framework should incorporate the following principles:

- Provide Clarity and Consistency on Definitions
    - Clarify definitions and distinctions of what constitutes an "alteration" and "forged maker" or "unauthorized signature" considering modern check fraud typologies, including "washed" checks, "cooked"/"baked" checks, and digitally altered signatures.
    - Ensure definitions are universally understood and in alignment with the UCC framework.
    - Clarify what constitutes an "original check" and "alteration" within the Presumption of Alteration considering modern check fraud typologies, including "washed" checks, "cooked"/"baked" checks, and digitally altered signatures.
- Support Efficient and Fair Loss Allocation
    - Maintain the principle that liability rests with the institution best positioned to prevent loss.
    - Balance responsibilities between depository and collecting banks, considering fraud-prevention capabilities, customer protection, and funds availability/return deadlines.
    - Facilitate cooperation between institutions by reducing the adversarial posture created by the current definitional gaps.
- Adapt to Evolving Fraud Methods
    - Incorporate flexibility to address new fraud methods and technologies without requiring wholesale regulatory overhaul.
    - Account for the practical challenges of identifying altered or counterfeit checks.

BPI has spent substantial time working with its members to evaluate definitions and solutions and are happy to participate in this effort.

3.6: Align Treasury Check funds availability timelines for consistency and streamline check return timelines

In response to the Agencies' question on shortening funds availability, we believe accelerating availability would give fraudsters quicker access to funds and reduce the time institutions have to investigate suspicious activity. It would also heighten cross-channel risks, as criminals could exploit the lag in check clearing against the instant, irrevocable settlement of wires, RTP®, or FedNow® transfers. Depository banks depend on fraud-detection tools and need sufficient time to review deposits and apply holds when warranted. Shortening deadlines would weaken these protections and increase fraud losses. Instead, the Agencies should allow banks to extend availability when a high likelihood of fraud exists (as outlined in item 3.3 above) while keeping standard timelines for the vast majority of checks.

Treasury check fraud continues to be a significant challenge for financial institutions, not just due to the rates of fraud, but also misaligned frameworks for funds availability and return obligations banks are subject to versus Treasury. Therefore, depositary banks would benefit from additional time to review Treasury checks before making funds available.[32]

Treasury has up to 60 days to determine whether a Treasury check bears a forged or unauthorized drawer's signature and to then reverse payment. In contrast, banks only have until midnight of the day following the day of presentment to pay or return a check. Treasury can also process a reclamation for a year and in some cases even longer. We recommend the Board, in collaboration with Treasury and other relevant bodies, explore regulatory solutions to shorten timeframes in which Treasury can automatically reverse payment on Treasury checks, encourage earlier identification of fraudulent government payments, and reduce associated losses for depository institutions. As Treasury moves toward eliminating Treasury check issuances in general, there will continue to be exceptions and by implementing these proposed changes, fraud involving the remaining check volume could be significantly reduced.

Although Treasury provides banks the ability to access Treasury's Treasury Check Validation Service (TCVS), banks typically accept the Treasury check for deposit processing before validating against the standalone TCVS system to determine if the Treasury check is on the list, if it matches as to the dollar amount, check number and payee name and the status of whether the check has already been paid. If it is not valid, the bank then needs to take action to hold the funds pending a return or reclamation claim from the Treasury. A better approach would be for Treasury to implement a positive pay with payee name process so that Treasury checks could be automatically returned upon presentment for payment, affording banks time to reverse any provisional credit to the deposit customer and saving Treasury the time and expense of processing a late return or reclamation.

Section IV: Payments Fraud Data Collection and Information Sharing

BPI appreciates the agencies' recognition that fraud mitigation requires not only strong bank controls but also a robust, data-driven ecosystem for understanding and responding to threats.

Information sharing of actionable fraud indicators in near-real-time is essential to disrupting fraud. There are various types of intelligence sharing that support different, but equally important, outcomes:

[32] Next-day availability for these checks is established by the Expedited Funds Availability Act, 15 U.S.C. § 4002(a)(2)(A), and statutory amendments may be necessary to extend the funds availability requirements for these checks.

- Fraud Data Sharing: Near-real-time exchange of account and transaction data linked to known fraud, enabling real-time prevention and decisioning.
- Intelligence Sharing: Timely, industry-wide sharing of emerging fraud types, trends, and tactics from authoritative sources to help institutions quickly adapt their defenses.
- Law Enforcement Collaboration: Coordinated escalation of large-scale fraud cases to law enforcement, shifting from isolated case reporting to systemic investigations aimed at dismantling organized networks.

Legal uncertainty continues to hinder information sharing. Institutions often avoid sharing certain information—even to protect the ecosystem—due to fear of litigation or liability. For example, when suspicious receiver accounts could be linked to first-party fraud, institutions may hesitate to warn peers, concerned it could be construed as triggering FCRA obligations.

While statutes like GLBA Section 313.15, the USA PATRIOT Act's Section 314(b), and other privacy exemptions permit certain fraud-related sharing, they lack clear safe harbor protections. Section 314(b) in particular is poorly suited for modern fraud collaboration and does not apply to cross-sector sharing with telecom or tech companies—despite their growing role in enabling fraud.

As many banks note, "nothing explicitly prohibits sharing, but nothing clearly permits it either." This legal gray area results in overly cautious behavior, missed opportunities to disrupt fraud, and unnecessary duplication of effort.

4.1: Establish Safe Harbors and Provide Clear Guidance for Fraud and Scam Information Sharing

The Agencies should work with Congress and other relevant authorities to establish clear legal authority and safe harbor protection for fraud-related data sharing. This includes enabling industries such as social media, telecommunications, and tech companies to share fraud information to protect consumers and reduce fraud. Legal certainty must extend to all parties acting in good faith to protect consumers and the payments system from fraud. To support these efforts, the Agencies can help by reinforcing the importance of robust fraud intelligence functions, much as they have long done with cybersecurity, while allowing banks the flexibility to design programs that fit their risk profile. Regulators can also encourage participation in established information-sharing groups such as FS-ISAC and NCFTA and help remove legal or operational barriers that may limit timely collaboration. The Agencies should support cross-industry efforts to improve fraud data and intelligence sharing across industries, not just within banking.

4.2: The agencies should work with industry to refine the FraudClassifier℠ and ScamClassifier℠ frameworks

A consistent fraud taxonomy is essential for identifying trends, guiding action, and improving information sharing. The Federal Reserve's FraudClassifier℠ and ScamClassifier℠ frameworks are important steps forward, but adoption across institutions has been inconsistent.

These models provide an excellent starting point for standard taxonomies. To enhance and update these models, the Federal Reserve should evaluate integrating emerging frameworks, such as the FS-ISAC Cyber Fraud Prevention Framework[33] or the Fraud Kill Chain[34], for more granular attack-stage analysis and mitigation planning. Coordination between industry and agencies to develop a unified, comprehensive

[33] FS-ISAC. (n.d.). *Cyber fraud prevention framework*. FS-ISAC.

[34] Fraud Kill Chain. (n.d.). *Fraud Kill Chain*.

taxonomy will help advance robust trend analysis and facilitate information sharing. The Agencies should also provide clarity on expectations regarding the use of these models by banks.

4.3: Leverage Suspicious Activity Reports (SAR) to generate more actionable and timely intelligence

In today's digital landscape, fraud attempts, particularly scams, are constant, high-volume, and generate a huge influx of SAR filings. In 2024, over 2.3 million SARS were filed by Depository Institutions related to fraud.[35] Banks devote significant time and resources to preparing SARs for fraud cases, creating an administrative workload that diverts resources from customer protection and prevention efforts. Banks receive little feedback on case outcomes, trends, or emerging indicators, that would bolster prevention efforts. This lack of feedback means that SARs function largely as a one-way reporting requirement rather than a collaborative prevention tool.

We recommend the Agencies work with FINCEN to provide feedback on the intelligence generated by these reports. FinCEN should produce and share regular, timely and actionable intelligence derived from SAR data – such as trends, typologies, and indicators – with reporting institutions. Greater dialogue would allow SAR filings to directly inform prevention strategies and support industry collaboration.

The Treasury Department and FinCEN have publicly acknowledged the need to modernize the BSA/AML regime, including SAR reform, to reduce unnecessary burdens and enhance usefulness for law enforcement.[36] Recent FinCEN notices and Treasury's Anti-Money Laundering/Countering the Financing of Terrorism (AML/CFT) National Priorities highlight the importance of improving data quality, streamlining reporting, and increasing feedback to filers. Aligning SAR requirements for payments fraud with these broader reform efforts would ensure that compliance obligations are proportionate to risk and more directly support prevention.

Section V: Reserve Banks' Operator Tools and Services

As the operator of critical payment systems, the Federal Reserve is responsible not only for ensuring system reliability but also for advancing tools that help participants detect and prevent fraud.

The Reserve Banks are uniquely positioned to identify network-level patterns and risks across all participating institutions. The ability for the Fed to share its wide visibility of fraud activity back to the payment system is critical. With that in mind we recommend the following:

- Provide network-wide risk scoring tools based on transaction activity across FedACH, Fedwire, and FedNow, enabling participants to assess the fraud risk of sending and receiving parties.
- Implement standardized fraud reporting for all transactions processed over Reserve Bank platforms to improve data aggregation, trend analysis, and targeted mitigation.
- Require transaction tagging using an agreed classification framework that includes payment flow (C2C, C2B, etc.), use case (eCommerce, bill payment, etc.), and industry segment (retail, financial services, etc.), enabling receivers to manage risk more effectively.
- Support Confirmation of Payee (CoP) across payment types, allowing consumers and businesses to verify recipient information before initiating payments—a proven measure in reducing authorized push payment (APP) scams internationally.

- Facilitate cross-rail fraud detection and insight sharing, especially where fraud typologies migrate between systems (e.g., ACH to FedNow) as tactics evolve.

By embedding these capabilities into the infrastructure it operates, the Federal Reserve can strengthen the security and integrity of its systems while setting a higher standard for fraud prevention across the payments ecosystem.

***

We appreciate the agencies' leadership and commitment to mitigating fraud in the payments system. Public-private partnership is key to achieving these goals, and we welcome the opportunity to discuss these recommendations further at your convenience.

Please do not hesitate to reach out to the undersigned by email at [redacted] if you have any questions regarding this letter, or if you would like to discuss further.

Respectfully submitted,

[redacted]

Gregory Williamson
Senior Vice President, Fraud Reduction Program
Bank Policy Institute | BITS