September 18, 2025

*Via Electronic Delivery*
Office of the Comptroller of the Currency
Board of Governors of the Federal Reserve System
Federal Deposit Insurance Corporation
400 7th Street SW Suite 3E-218
Washington, DC 20219

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 Consumer Bankers Association (CBA) [1] appreciates the opportunity to respond to the joint request for information (RFI) issued by the Office of the Comptroller of the Currency (OCC), the Federal Reserve Board (FRB), and the Federal Deposit Insurance Corporation (FDIC) regarding potential actions to address payments fraud.[2] CBA shares your concerns over the harms that fraud and scams inflict on consumers, businesses, and financial institutions. CBA's members are committed to defending consumers from bad actors, including the threat of increasingly sophisticated scammers targeting Americans. CBA and its members support efforts that advance common sense, pragmatic strategies that get to the root of these global problems, which are only growing in frequency, prevalence, and severity.[3]

Last summer, CBA contributed to the publication of a white paper exploring how industries could work together and with government to prevent fraud and other harms against consumers and businesses, "Stopping Scams Against Consumers: Roadmap for a National Strategy."[4] CBA subsequently convened a fraud and scams roundtable[5] on July 17, 2024, bringing together leaders from the White House, government agencies, law enforcement, including the FBI, and other private sector industries, including

[1] The CBA is a member-driven trade association, and the only national financial trade group focused exclusively on retail banking—banking services geared toward consumers and small businesses. As the recognized voice on retail banking issues, CBA provides leadership, education, research, and federal representation for its members. CBA members operate in all 50 states. They include the nation's largest bank holding companies as well as regional and super-community banks. Eighty-three percent of CBA's members are financial institutions holding more than $10 billion in assets.
[2] Request for Information on Potential Actions To Address Payments Fraud, 90 Fed. Reg. 26293 (Jun. 20, 2025), *available at* https://www.govinfo.gov/content/pkg/FR-2025-06-20/pdf/2025-11280.pdf.
[3] *See, e.g.*, Press Release, FTC, FTC Data Show a More Than Four-Fold Increase in Reports of Impersonation Scammers Stealing Tens and Even Hundreds of Thousands from Older Adults (Aug. 7, 2025), *available at* https://www.ftc.gov/news-events/news/press-releases/2025/08/ftc-data-show-more-four-fold-increase-reports-impersonation-scammers-stealing-tens-even-hundreds.
[4] Nick Bourke, Stopping Scams Against Consumers: Roadmap for a National Strategy (Jul. 17, 2024), *available at* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4897644.
[5] Press Release, CBA, Fraud and Scams Roundtable – Summary and Proposed Next Steps (Jul. 24, 2024), *available at* https://consumerbankers.com/press-release/icymi-cba-convenes-cross-industry-public-private-roundtable-to-inform-whole-of-government-approach-to-combat-fraud-and-scams/.

telecommunications, fintechs, and non-profit consumer organizations to discuss the white paper. The U.S. Government Accountability Office (GAO) also recently issued a report entitled "Consumer Protection: Actions Needed to Improve Complaint Reporting, Consumer Education, and Federal Coordination to Counter Scams"[6] (the GAO Report), which identified and explored many of the same topics covered in the white paper and roundtable.

As noted in the white paper, roundtable, and GAO Report, the threat environment is consistently evolving, and one thing has become abundantly clear in light of the innovations by these malicious actors: no single institution or industry has the capabilities to unilaterally address this problem. Indeed, no single private industry sector can look across all sectors and gather the data and information required to fully assess the magnitude of the problem, detect and report rising fraud vectors or scam schemes, or track perpetrators. While critical elements of the payment ecosystem can be modernized, fighting fraud and scams requires a whole-of-society approach that goes beyond banks alone. In particular, other parties that provide the tools for scammers to contact their victims, including social media platforms, telecommunications providers, online platforms (including search engines), and other technology providers, must be equally active participants in fighting fraud and scams.

For example, insights from social media companies about how users are interacting with fraudulent ads, paired with information about the behaviors and actions of scammers operating on social media, would help parties understand how and where these crimes are proliferating. By bringing together what social media companies see with what customers report to their financial institutions, both sides could better identify bad actors, protect customers, and be nimbler in addressing emerging trends. These efforts will require action beyond the reach of the banking agencies, collaborating with other authorities with oversight over these upstream entities. CBA urges these agencies to lead the way by coordinating a plan to fight fraud and scams across all sectors.

CBA thus applauds the prudential regulators' decision to solicit feedback on the scope of the problem, as well as on what the agencies individually or collectively can do in their varying roles to help stymie the tide of fraud and scams. CBA recommends:

- The government facilitates a cross-sector, public-private collaboration for fighting fraud and scams that ensures all relevant parties bear the necessary obligations and that there is adequate prosecution of fraud and scam activity.
- Regulators provide sufficient supervisory guidance and regulatory clarity on payments fraud detection, prevention, and mitigation efforts.
- A nationally coordinated fraud awareness campaign is needed for disrupting fraud and scams schemes by informing consumers on how to identify and

[6] GAO, *GAO-25-107088 – Consumer Protection: Actions Needed to Improve Complaint Reporting, Consumer Education, and Federal Coordination to Counter Scams* (Apr. 8, 2025), *available at* https://www.gao.gov/products/gao-25-107088?utm_campaign=usgao_email&utm_content=topic_bizregs&utm_medium=email&utm_source=govdelivery.

respond to such schemes.
- Industry needs to advance an accepted industry-wide standard and fraud and scam taxonomy, supported by standardization efforts by regulators, to promote consistent and reliable data collection to support countering fraud and scams.

Please find below CBA's responses to individual questions in the RFI.

* * *

## External Collaboration (Questions 1-4)

### Q1. What actions could increase collaboration among stakeholders to address payments fraud?

To truly safeguard Americans and combat malicious actors, a coordinated effort across public and private entities is essential. The telecommunications industry, social media platforms, technology firms, federal agencies, national security officials, law enforcement, and the entire financial services sector need to advance solutions in partnership, as no single industry or sector has the capabilities to disrupt these criminal enterprises alone. Regulators must be aware of the end-to-end landscape of how fraud and scams occur, rather than focusing solely on the end transactions within the financial services sector. Fraud and scams proliferate via telecommunications, social media, and online platforms, well before a financial transfer is even made. The ease with which fraudsters can impersonate banks, government agencies, celebrities, and even family members makes combatting these scams an ever-changing task. In fact, the Federal Trade Commission (FTC) has recently spotlighted that there has been a more than four-fold increase since 2020 in reports from older adults who say they lost $10,000 or more to scammers impersonating government agencies or businesses.[7] As the FTC's report noted, "combined losses reported by older adults who lost more than $100,000 increased eight-fold, from $55 million in 2020 to $445 million in 2024."[8] Many of the recommendations throughout this letter – especially those for Q3 regarding engagement with other industries, Q4 regarding adequate prosecution and penalties for fraudsters and scammers, and Q16 regarding data sharing to counter fraud and scams – would benefit from legislation and subsequent regulations to meaningfully affect change.

Moreover, regulators beyond the prudential regulators, including the Consumer Financial Protection Bureau and regulators *outside* of the financial services sector, must take care to avoid unintentionally negatively impacting industry's efforts to fight fraud and scams. For example, the Federal Communications Commission's (FCC) Draft

[7] FTC, *supra* note 3, *available at* https://www.ftc.gov/news-events/news/press-releases/2025/03/new-ftc-data-show-big-jump-reported-losses-fraud-125-billion-2024.
[8] *Id.*

Consent Revocation Order (Draft Order)[9] risked undermining consumer safety and many of the critical fraud prevention efforts undertaken by banks. As CBA summarized for the FCC,[10] the Draft Order did not sufficiently distinguish between these vital communications and other types of robocalls, creating a serious risk that consumers could inadvertently revoke consent for fraud alert, and without an explicit carveout for fraud-related notifications, banks may be forced to limit or eliminate these alerts due to compliance uncertainty in sending these messages as "exempted," leaving consumers more vulnerable to financial crimes.

Collaboration is an important starting point, and already underway with efforts such as the Aspen Institute's Task Force on Scam and Fraud Prevention,[11] but further steps are needed. Within the financial services sector, various payment channels have disparate systems to report fraud, which may result in partial mitigation while not fully eliminating the ability for fraud to continue through a specific account or individual. To address this, the federal government, alongside industry, can immediately focus on developing a single secure industry-wide, real-time information sharing platform that enables immediate notification of fraudulent or collusive customers or merchants. Such a platform will help deconstruct silos and disrupt bad actors, reducing their effectiveness. Such a platform may require additional clarity from regulators, as it may be unclear what information industry participants are and are not allowed to share, as well as what actions are needed to share such information securely, overcoming privacy concerns for example. Regulators can also explore the possibility of a safe harbor or liability protections for institutions that are sharing such information in good faith when attempting to identify and prevent a fraud or scam. Addressing the aforementioned aspects of the platform, as well as determining the appropriate division of management of the platform itself among industry and the federal government, will necessarily require further engagement and discussion.

**Q2. 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?**

Within the financial services industry, collaboration on and the establishment of uniform fraud reporting standards to enable common terminology and definitions across the financial services industry would enable improved data quality and insights into emerging trends at a faster pace. To that end, restrictions that impact information sharing among industry participants, such as data privacy laws and requirements under the Fair Credit Reporting Act (FCRA), should be reexamined with a lens toward

[9] *Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991*, CG Docket No. 02-278, Report and Order and Further Notice of Proposed Rulemaking, FCC-24-24A1 (Feb. 16, 2024), *available at* https://docs.fcc.gov/public/attachments/FCC-24-24A1.pdf.
[10] CBA, *Letter re: Concerns Regarding the FCC's 2024 Draft Consent Revocation Order and Its Impact on Fraud Prevention Efforts* (May 29, 2024), *available at* https://consumerbankers.com/wp-content/uploads/2025/06/CBA-TCPA-Consent-Revocation-Order-Letter-FCC-1.pdf.
[11] *See, e.g.*, Aspen Institute Financial Security Program, Phase One Working Group Outputs (May 23, 2025), *available at* https://fraudtaskforce.aspeninstitute.org/phase-one-outputs.

promoting fraud prevention, including offering safe harbors for sharing of information regarding fraud and scams where appropriate.[12] Collaboration with industries outside of the banking industry are further discussed in Q3.

**Q3. 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?**

Combatting frauds and scams must be a whole-of-government, cross-sector, public-private collaboration. CBA encourages the regulators, through their role on Financial Stability Oversight Council (FSOC), to work with Treasury—who can then work with other Departments and Agencies, like the Department of Justice and the FTC, to reduce frauds and scams, promoting American innovation, and protecting our consumers. For example, collaboration with (i) social media companies and (ii) telecommunications sector is vital for a holistic and successful approach to fighting fraud and scams. Each of those collaborative efforts are discussed in turn below:

*Social Media Industry*: Meaningful process in combatting fraud and scams can be made through collaboration with social media companies, particularly in light of the fact that many of these schemes originate on such platforms. Some banks have reported that nearly half of Zelle scam transactions originated via social media contact, a figure consistent with the broader trends highlighted in a June 11, 2025 letter signed by 42 bipartisan Attorneys General highlighting the rapid proliferation of scams on social media platforms.[13] That letter shares examples of "pump-and-dump" schemes in which scammers are placing ads on Facebook "that impersonate prominent figures, such as Warren Buffett, claiming to offer high returns on investments." Beyond these so-called "pump-and-dump" tactics, scammers are also advertising fake goods and services[14] to steal payment credentials and money, sometimes impersonating legitimate businesses and offering deals at too-good-to-be-true prices. Scammers further use social media to build relationships with unsuspecting victims, emotionally manipulating them into sending financial resources through romance scams. In the future, as artificial intelligence (AI) becomes more sophisticated, industry anticipates a significant increase

---

[12] *See, e.g.*, CBA, et al., *Joint Financial Trades Response to the House Financial Services Committee Request for Information on Current Federal Consumer Financial Data Privacy Law and Potential Legislative Proposals* (Aug. 28, 2025) ( "Finally, to give an example of the kinds of amendments that could be uniquely considered for [the Gramm-Leach-Bliley Act (GLBA)] as compared to a comprehensive privacy law, GLBA could be amended to include a safe harbor for the sharing of information regarding fraud and scams. Today, financial institutions can be limited in their ability to share information, both with each other and with law enforcement, which hampers both government and industry efforts to prevent bad actors and better protect consumers.").

[13] Press Release, Office of the New York State Attorney General, Attorney General James Leads Bipartisan Coalition Urging Meta to Protect Users from Fraudulent Investment Ads (Jun. 11, 2025), *available at* https://ag.ny.gov/press-release/2025/attorney-general-james-leads-bipartisan-coalition-urging-meta-protect-users.

[14] Jeff Horwitz and Angel Au-Yeung, Meta Battles an 'Epidemic of Scams' as Criminals Flood Instagram and Facebook, The Wall Street Journal (May 15, 2025), *available at* https://www.wsj.com/tech/meta-fraud-facebook-instagram-813363c8.

in the effectiveness of these scams if action is not taken to address them now. To that end, addressing scams that originate on social media will require additional obligations for social media companies to comply with to protect consumers, which could include:

- Implementing standards similar to "Know Your Customer" (KYC) requirements to identify scam advertisers, accounts, and repeat offenders;
- Blocking offshore advertisers from targeting U.S. consumers where scam risk is present based on location;
- Removing impersonated profiles, fraudulent ads, and scam marketplace listings within a certain number of business days of identification;
- Blocking bad actors from participating on the platform within a set period of business days after the determination of scam activity;
- Establishing consumer alert mechanisms for suspected scam content, such as direct messages or links to external sites;
- Requiring reporting of confirmed scam activity to a national registry and to law enforcement within a certain number of business days; and
- Creating a standardized, cross-platform reporting mechanism to allow consumers to report scam activity that appears across multiple social platforms.

*Telecommunications Industry*: Collaboration with the telecommunications industry is also vital. Some of CBA's member banks have actively engaged with the telecommunications providers to prevent spoofing of bank phone numbers. Such collaborations, though, have highlighted the gaps and limitations that still exist in this space. Caller ID spoofing has been a persistent and pernicious attack vector over time. Bad actors can manipulate the information that appears on phone screens when calling, making it appear as though they are calling from their target's bank, often under the pretense of protecting them from fraud. Taking advantage of the implicit trust conveyed by a purported bank-owned phone number showing up on the Caller ID, the bad actors will then try a range of tactics for monetizing the attack, including getting the customer to provide their login credentials, provide a one-time PIN, send a Zelle payment, or mail a debit card. Up until the past year, there was no way for a bank to protect its own phone numbers from being spoofed in this manner. After years of discussions and raising this issue with various telecommunication carriers, there are finally new, fee-based services available for addressing this issue. Banks may now use this new service to protect bank-owned phone numbers from being spoofed by bad actors. As a result, on an annualized basis, banks have blocked millions of spoofing attempts against bank numbers. However, this approach only allows banks to protect *their own phone numbers* and *only for phone calls*. There is currently no way to prevent spoofing of text messages. Addressing scams that originate with telecommunications providers will require stronger obligations for such providers, which could include:

- Requiring robust international anti-scam filters to prevent spoofing and mass fraud attempts;
- Establishing scam reporting and prevention methodologies similar to those that allow consumers to report and prevent spam communications;

- Verifying the authenticity of all messages and calls originating from outside the United States and alert consumers in real time;
- Complying with and expanding on STIR/SHAKEN protocols to verify caller IDs, stricter enforcement of falsely attesting to STIR/SHAKEN level of calls, and prohibiting SIM swapping and unauthorized number porting;
- Ensuring major carriers enforce anti-fraud standards for mobile virtual network operators that lease their networks;
- Creating mechanisms to share confirmed scam numbers and traffic data across carriers and report confirmed actors to law enforcement within a set number of business days; and
- Developing stronger regulations tying a business or personal identity to a phone number to prevent the abuse of "disposable" phone numbers.

CBA would also note that the following entities may have a role to play in fighting fraud and scams and can be considered in connection with the aforementioned collaboration opportunities:

- Advocacy groups, who can provide insights into identifying scam vulnerability and may be better suited to educating specific communities;
- Consulting firms, particularly those with significant forensic teams;
- Cross-sector, public private initiatives like the Aspen Institute;
- Financial technology companies and internet service providers, which may provide financial crime and/or anti-fraud offerings;
- Organizations commonly involved in the depletion of fraudulent funds (e.g., casinos, peer-to-peer payment providers, cryptocurrency platforms)
- Payment networks, such as Nacha, Mastercard, Visa, etc.;
- Psychologists, who can provide keen insights into identifying scam vulnerability;
- Vendors and non-profit organizations with expertise in cyber solutions and security; and
- The AI industry, which can educate consumers and the financial industry on how to best detect their tools when used in scams and fraud.

**Q4. Could increased collaboration among Federal and State agencies help detect, prevent, and mitigate payments fraud? If so, how?**

Domestically, law enforcement agencies need to have the centralized tools to track fraud and share information, which could help law enforcement and industry alike identify prevalent activity and criminal activity much sooner. Increased visible enforcement actions, along with strong prosecution against criminals, particularly in connection with check fraud, will hopefully serve as a deterrent for future fraudulent activities. Law enforcement can also explore: (i) formal channels to assist in funds recovery; (ii) engagement with credit reporting agencies and vendors to identify instances in which social security numbers are used to open accounts in different states; (iii) monitoring of the dark web and fraud-as-a-service providers; (iv) investigating limited liability companies that are suspected of having been opened for fraudulent purposes; and (v)

working to develop a centralized Federal office for anti-fraud activity to coordinate the Federal efforts to fight fraud and scams. These efforts will require dedicated resources, and ongoing collaboration with Congress to ensure agencies are properly equipped to prevent and mitigate payments fraud.

Law enforcement should also explore any collaborative opportunities to pursue organized crime and transnational groups seeking to exploit consumers through scams. Indeed, these scam activities are perpetrated by globally-networked criminal organizations, as vast networks of underground scam syndicates now operate in South-East Asia, Africa, Eastern Europe, the Middle East, and South America.[15] Many of these organizations use forced labor sourced via transnational human trafficking pipelines, with the United Nations estimating that, in 2023, upwards of 220,000 people were being forced to work against their will as scammers in Myanmar and Cambodia alone. The ill-gotten profits these organizations churn out —often at the expense of unsuspecting U.S. consumers —have been traced to foreign state actors and global crime syndicates.[16] Law enforcement must be cognizant of the domestic impacts these international organizations are having on Americans, and explore all collaborative options for prevention of these crimes and prosecution of their perpetrators.

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

### Q5. 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?

An effective fraud education strategy must be multi-faceted, targeted, and continuously evolving to meet the growing sophistication of financial crime. Education efforts are most impactful when delivered at key touchpoints—such as onboarding, product discussions, and annual reviews—using direct prompts that require user acknowledgment (e.g., "I agree" or "I understand") to introduce *smart* friction that creates meaningful pauses, which can prompt consumers to reconsider potential fraud risks. Real-time, personalized education from trusted banking professionals remains the most effective – yet the least scalable – method, especially in combating rapidly shifting fraud tactics and misleading social narratives that downplay the harm of scams.

Industry-wide collaboration is also critical. Industry partners benefit from specialized, advanced ongoing education regarding payment frauds from other peers involved in payments fraud, including those outside of their direct industry to obtain a more holistic

[15] *See, e.g.*, The Vast and Sophisticated Global Enterprise That Is Scam Inc., The Economist (Feb. 6, 2025), *available at* https://www.economist.com/leaders/2025/02/06/the-vast-and-sophisticated-global-enterprise-that-is-scam-inc.
[16] Press Release, U.S. Department of the Treasury, Treasury Sanctions Burma Warlord and Militia Tied to Cyber Scam Operations (May 5, 2025), *available at* https://home.treasury.gov/news/press-releases/sb0129.

view of the lifecycle of fraud end-to-end. Partnerships with organizations like the Better Business Bureau (BBB) Institute for Marketplace Trust and education nonprofits have led to valuable tools such as the BBB Scam Tracker, which helps consumers better identify and report scams, and the Scam Survivor Toolkit, which provides personalized recovery plans to scam survivors. Many banks also have longstanding partnerships with education nonprofits that offer free resources, such as free online financial literacy courses. Taken together, these actions reflect the unwavering commitment to protecting consumers from financial crimes and industry's relentless drive to identify and thwart the bad actors who seek to exploit them.

However, a broader, nationally coordinated fraud awareness campaign—similar in scale to Smokey Bear's wildfire prevention effort—is needed to reach diverse audiences and shift public perception. Fraudsters' continually evolving schemes are enhanced by ongoing rhetoric that characterize financial institutions, which are trying to protect their consumers, as focused solely on fees or profits or as easily susceptible targets for "harmless" financial hacks or schemes that originate on social media. Ultimately, while effective resources already exist, the challenge lies in connecting consumers with these tools before they become victims, requiring ongoing innovation, cross-sector collaboration, and a more holistic understanding of fraud's lifecycle. New solutions and partnerships are also needed, especially at a time when more of these financial crimes are originating overseas from global crime syndicates.[17]

**Q6. 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?**

Maintaining consumer awareness of how to identify and respond to frauds and scams is crucial to disrupting these schemes and reducing their effectiveness. However, there is a potential risk of alert/education fatigue, whereby repeated messaging can cause consumers to "tune out" of this important messaging. To sustain the impact of consumer awareness education efforts, it is integral for the education to be tailored to specific populations and for messengers to continually explore new communication strategies to ensure the content remains relevant and engaging. Education should also have the explicit goal of raising attention to populations who may not be aware of these increasing threats, in addition to educating those familiar with the latest criminal tactics.

**Q7. Which approaches could make existing payments fraud education more effective? For example, would targeting outreach to particular audiences or**

[17] *See, e.g.*, Huizhong Wu, Jintamas Saksornchai, and Martha Mendoza, They were forced to scam others worldwide. Now thousands are detained on the Myanmar border, AP (Mar. 9, 2025), *available at* https://apnews.com/article/myanmar-thailand-scam-centers-trapped-humanitarian-c1cab4785e14f07859ed59c821a72bd2?utm_source=openbanker.beehiiv.com&utm_medium=referral&utm_campaign=banks-are-fighting-fraud-and-scams-but-we-can-t-do-it-alone.

**conducting additional education in collaboration with other key stakeholders be effective?**

Education is critical to combatting scams and fraud, yet current efforts are often overlapping, incomplete, or too small to scale. An effective fraud education approach should start with the audience in mind: identifying who needs to hear the message, how they process information, and what will capture their attention. In a world overflowing with alerts, tips, and warnings, the challenge is not just sharing information, but making it resonate and stick. Build a fraud campaign like it's a public health campaign, driving sustained public awareness efforts, expanding recognition of fraud awareness months, and establishing a core, universal message that is clear, memorable, and actionable. Campaigns should be repeated and reinforced across multiple channels, including social media, videos, email, online and print ads. Cross-sector collaboration is essential to ensuring effective fraud education. Bringing together financial institutions, government agencies, law enforcement, and community organizations to blend perspectives and amplify reach. Federal agencies can support the industries by sponsoring the development and maintenance of a national campaign.

In addition, real stories hold a profound weight in making the threat of scams tangible for people, especially in cases where someone thinks they'd never fall for a scam. Lastly, a data-driven approach should guide priorities, ensuring education efforts are targeting the highest risk demographics and fraud types, with measurable outcomes to track success. At a national level, a centralized government-led education plan would unify these efforts by providing standardized education materials that organizations can customize and give consumers practical tools to spot and respond to scams. By combining a strong government-led approach, impactful messaging, fraud education can become more effective, trusted and difficult for bad actors to target Americans.

**Q8. Are current online resources effective in providing education on payments fraud? If not, how could they be improved?**

While there are some payments fraud education resources – such as Safe Banking for Seniors,[18] a free national program sponsored by the American Bankers Association that provides bankers with tools and resources to connect with their local communities on certain topics, and "Banks Never Ask That,"[19] an education campaign delivered through social media designed to help consumers be aware of common scam tactics – locating and curating all available materials can be challenging and time-consuming for users, reducing overall effectiveness. Additionally, the average consumer may struggle to differentiate between credible fraud education resources, like those mentioned above, and outdated or sensationalized content. Payments fraud education could be significantly improved through centralized curation by an industry consortium or a

[18] American Bankers Association, Safe Banking for Seniors, *more information available at* https://www.aba.com/advocacy/community-programs/safe-banking-for-seniors.
[19] American Bankers Association, Banks Never Ask That, *more information available at* https://www.banksneveraskthat.com/.

government body. Furthermore, educational materials should be tailored to accommodate audiences with varying levels of time, interest, and familiarity with the subject. Most importantly, to ensure their effectiveness, educational efforts must avoid overwhelming consumers with excessive information and evolve to match the changing strategies of scammers.

## Regulation and Supervision (Questions 9-15)

### Q9. 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?

Increasing regulatory or supervisory actions could hinder tactics banks employ to combat fraud and scams. Fraudsters are constantly developing new techniques, requiring financial institutions to be dynamic and implement creative solutions to combat ongoing threats effectively. While regulation and supervision remain important, regulatory frameworks risk stifling innovation at the very time when it is most needed. New requirements must be carefully designed and introduced in a way that supports, rather than blocks, industry-led efforts. The agencies must work collaboratively with the banking industry to streamline supervisory practices and modernize key regulatory definitions and authorities. Doing so would provide financial institutions with the flexibility needed to address both existing and emerging fraud threats—and to protect the consumers and systems most at risk.

As fraud risks grow and faster payments expand, banks need regulatory flexibility to detect and pause suspicious transactions in real time. Currently, the Expedited Funds Availability Act (EFAA) and Regulation CC only allow extended holds for check deposits, not for electronic payments like wires, ACH, or FedNow. This limits banks' ability to temporarily hold and review suspicious electronic deposits, especially in scam scenarios. While some banks use fraud detection tools for electronic payments, there is no clear regulatory authority to pause or return suspicious funds before they are credited. Account-level restrictions are often used to prevent further losses, but investigations are complex and regulatory uncertainties such as conflicting examiner guidance and UDAP/UDAAP concerns—discourages banks from applying holds, even to protect consumers. Banks should be allowed to place extended holds on electronic deposits suspected of fraud, without violating Regulation CC's next-day availability rule. Regulators should ensure that expedited funds availability laws work alongside fraud prevention and anti-money laundering requirements.

Bipartisan legislative actions also offer a path to stronger defenses against fraud and scams. The "Task Force for Recognizing and Averting Payments Scams (TRAPS) Act,"[20] introduced by Senator Mike Crapo (R-Idaho) and Senator Mark Warner (D-VA), would establish such a task force to formally coordinate efforts, develop best practices, and recommend comprehensive solutions. The TRAPS Act would create such a formal structure for collaboration to make the entire financial ecosystem safer for consumers. Recognizing the urgent need to address fraud and scams representatives Zach Nunn (R-Iowa) and Jim Himes (D-CT) introduced the House companion bill to the TRAPS Act[21]. Similarly, representatives Zach Nunn (R-Iowa) and Josh Gottheimer (D-N.J.) introduced the "Guarding Unprotected Aging Retirees from Deception (GUARD) Act."[22] If enacted, this legislation would direct federal agencies to report to Congress on the current state of fraud and scams. In a recent op-ed, CBA President and CEO Lindsey Johnson highlighted the need for a whole-of-government approach to combat fraud and scams and urged lawmakers to pass recently introduced legislation to do so: "This level of transparency will not only bring light to the magnitude of the crisis but also drive greater accountability across the public and private sectors alike. This legislation is a step in the right direction and provides a tangible example of how policymakers in Washington can advance sound policy to protect Americans. By publicly disclosing the scale of the issue, the GUARD Act would shed light on vulnerabilities and weaknesses across the consumer ecosystem to better inform and enable solutions at a level not possible today."[23]

Sophisticated criminal networks are waging a multi-front war against the American consumer —not just within the payments system but across every mode of modern communication and commerce. By uniting government, law enforcement, and the private sector to craft multi-sector solutions, the GUARD and TRAPS Acts represent a meaningful step forward in addressing this critical challenge.

**Q10. 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?**

---

[20] S. 2019, "A bill to establish a Task Force for Recognizing and Averting Payment Scams, and for other purposes" or "TRAPS Act," 119th Cong. (2025), introduced Jun. 10, 2025, *available at* https://www.congress.gov/bill/119th-congress/senate-bill/2019.

[21] H.R. 4936, "A bill to establish a Task Force for Recognizing and Averting Payment Scams, and for other purposes" or "TRAPS Act," 119th Cong. (2025), introduced Aug. 08, 2025, *available at* https://www.congress.gov/bill/119th-congress/house-bill/4936/text.

[22] H.R. 2978, "Guarding Unprotected Aging Retirees from Deception Act" or "GUARD Act," 119th Cong. (2025), introduced Apr. 21, 2025, *available at* https://www.congress.gov/bill/119th-congress/house-bill/2978.

[23] Lindsey Johnson, Sadly, the scammers are winning — but our government can help, The Hill (Apr. 30, 2024), *available at* https://thehill.com/opinion/finance/5273422-government-strategy-fraud-scams/.

Current supervisory guidance on payments fraud detection, prevention, and mitigation could be modernized and strengthened to address gaps in liability and transaction handling. Regulatory agencies should partner with the banking industry to streamline supervisory practices and update essential regulatory definitions and authorities, allowing banks to adopt a flexible, risk-based approach to both current and emerging threats. Future guidance and/or rulemakings should establish a shared liability framework to clarify responsibilities among all stakeholders in the fraud ecosystem, including telecommunications providers, digital asset industry, non-bank financial service providers, and social media companies. It should also provide clarity and certainty on safe harbors and liability protections for institutions acting in good faith, such as holding funds or closing accounts. Finally, guidance should address the management of authorized push payment transactions, in which customers victimized by imposter scams authorize a transaction resulting in different liabilities depending on the method of payment used.

No payment method is foolproof and electronic payment methods, while significantly more secure than paper checks, are still susceptible to fraud. First party fraud, although not as prevalent of an issue as third-party fraud, is growing in mature payment methods like ACH debit and credit. ACH debit was originally designed to be used for consumers to pay recurring bills but has evolved over the years to also be used by businesses for one off commerce and third-party wallet funding purposes. ACH credit has seen evolving fraud techniques including an increase in false claims of fraud even when ACH links have been validated. The evolution of ACH has occurred without any significant update to Nacha rules, which in turn can result in losses for the financial system. Because of the growing number of transactions using ACH debit and credit, it is worthwhile for the federal agencies to urge payment networks like Nacha to review whether the underlying use cases are “fit for purpose” under their existing rules and operational frameworks and update their rails with fraud mitigating controls.

**Q11. How might new or revised supervisory guidance assist small community banks in detecting, preventing, and mitigating payments fraud?**

N/A

**Q12. What is the experience of consumers and businesses when supervised institutions place holds on depositors' funds because of suspected payments fraud?**

**(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?**

The experience for consumers and businesses can vary significantly depending on the payment channel and the specific fraud control framework used by each institution. The

portion of transactions affected by holds, delays, or account freezes varies from 1% to as high as 6%, including cases where customers can "self-clear" a transaction through step-up authentication, reducing delays. The frequency and impact can depend greatly on the institution's controls to prevent and interdict fraud, and overall success rate in identifying fraudulent activity.

**(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?**

While SAR confidentiality rules do not prohibit financial institutions from disclosures about held funds, they *do* prohibit financial institutions from disclosing a SAR filing or information indicating whether or not a SAR has been filed to customers and other parties. As such, privacy requirements, rather than SAR confidentiality rules, are the more relevant hurdle preventing financial institutions from communicating with fraud victims that funds have been held in a customer account.

**Q13. 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?**

CBA supports actions that would help transition the industry to more secure and modern payment methods, including clarifying that although the exceptions in Regulation CC may not apply to electronic payments, other fraud-related and AML obligations may supersede the obligation to provide next-day availability. More flexibility under Regulation CC to implement better check fraud guardrails, such as expanding exception holds for checks based on fraud risk and expanding the definition and scope of "new account" exception holds, would support investment in the future state of payments balanced with necessary consumer protections.

Today many depository institutions use the Uniform Commercial Code to govern their response to interbank disputes involving check fraud, and there are clear timelines for consumers to report fraudulent check transactions. However, guidance governing the processing of these claims between institutions lack consistent definitions and specific timelines for certain types of claims, which can lead to confusion, extended claim handling times, and significantly delay recoveries. There are also disparities in the types

of documentation banks require for disputes and how disputes are submitted. For example, some banks require items to be mailed or sent via fax.

Industry would benefit from clear, simplified, and reasonable guidance on consistent terminology, timelines for submitting (including evidentiary standards), handling, and responding to claims, as well as standards for specific claim types to reduce the likelihood of dispute or arbitration. Such timelines should also incorporate the modern reality that investigations often rely on instantaneously shared images, rather than physically transported documents. The most common scenarios this occurs are when a claim of a material alteration or forged endorsement is received. The investigations are made even more difficult in the modern era when electronic images of varying quality, rather than physical checks, are the items examined. Further, there should be a reevaluation of whether notification letters must be mailed or whether digital channels can be leveraged for delivery. CBA recommends the agencies collaborate with industry to resolve these ambiguities and inconsistencies, as well as to improve and expedite claims processing.

**Q14. 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?**

It is vital that funds availability acknowledge the modern reality of increasingly sophisticated fraud and scams activity. In light of these developments, CBA recommends that: (i) the time by which funds must be made available after a deposit to a new account be lengthened beyond their current requirements; (ii) institutions be able to make a lower amount of funds available on the first business day after a deposit and be able to make a greater amount of the funds available at a later date; and (iii) institutions be able to withhold greater amounts if a check has been returned in the past. These changes will afford institutions additional time to identify suspected payments fraud and help slow down the rampant rate of fraud activity. More broadly, in light of the rampant increase in check fraud, exacerbated by the increasing ease with which fraudsters can manipulate documents, CBA reiterates the need to transition to more secure and modern payment methods.

**(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?**

While some industry technological advances exist, these advantages may only be a benefit if an institution is a member of a consortium. Shortening the requirements for Regulation CC, in conjunction with continued increased funds availability requirements, will elevate financial losses. Such changes may also necessitate industry adopting more

conservative approaches, which can stymie industry technological advancements and growth.

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

Shortening funds availability requirements will lead to increased losses, particularly absent any other changes to mitigate the risk faced by institutions. Reducing the time institutions, consumers, and businesses must identify, report, and mitigate the risk of loss related to fraudulent activity will correlate to an increase in payment fraud attempts and losses experienced by victims, as these changes will allow fraudsters and scammers to perpetrate and profit from their crimes before they can be identified and stopped.

**(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?**

In connection with the expeditious return requirement, CBA recommends that any changes promote greater alignment and industry standards on return types and definitions. For example, one institution may characterize a check as "altered" whereas another classifies the same check as "counterfeit." This issue is magnified when only the image of a check, rather than the paper check itself, is reviewed. Clear and consistent standards developed in collaboration with the banking industry will promote efficient fraud prevention efforts.

**Q15. 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?**

Yes, depository institutions would benefit from further clarification on the appropriateness of invoking exceptions. Regulation CC's exception provisions do not fully mitigate the risk of check fraud for specific scenarios when an institution suspects fraud. Additionally, some depository institutions have real-time fraud checks and funds availability, whereas other depository institutions must wait until the next day. Finally, there are ambiguities over the process to notify clients of Regulation CC holds, particularly over whether the notice can be electronic as compared to delivered via a

written letter. Providing clear guidance to institutions on these issues can mitigate risk without necessitating more disruptive fraud mitigation activities, such as account level restrictions.

## Payments Fraud Data Collection and Information Sharing (Questions 16-20)

### Q16. Broadly, how could payments fraud data collection and information sharing be improved?

Data collection and information sharing in the fraud and scam space is an area that should be significantly improved, yet it remains one of the most difficult challenges to address. Data sharing barriers include inconsistent data points, staff turnover at financial institutions, lack of agreement on how to indemnify partner financial institutions when sharing data, unclear governance on what data can be shared, and the complexity of offering in a rapidly evolving payments landscape. The FraudClassifierSM[24] and ScamClassifierSM[25] models represent a strong first step in defining and refining the national conversation around fraud and scams, the creation of an accepted industry standard and fraud & scam taxonomy that meets the needs of both large and small institutions, would allow for more consistent and reliable data collection. At the same time, fragmented state and federal privacy approaches present ongoing challenges to consistent data sharing. Information sharing should be cross-sector and in real-time, to be most effective in comprehensive fraud and scam prevention, and should be incentivized with clear legal authority and safe harbor protections to overcome privacy and liability concerns.[26]

### Q17. 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?

Barriers to the collection and sharing of payments fraud data between industry largely stem from the lack of standardization regarding what information can be shared and what the requirements of participation are between industry and stakeholders. Without a consistent baseline for reporting and participation, financial institutions are left to navigate different interpretations of data-sharing obligations. Additionally, challenges may arise from existing entities (e.g., Verafin) which already collect fraud data. These

---

[24] The Federal Reserve, FraudClassifierSM Model, *more information available at* https://fedpaymentsimprovement.org/strategic-initiatives/payments-security/fraudclassifier-model/.
[25] The Federal Reserve, ScamClassifierSM Model, *more information available at* https://fedpaymentsimprovement.org/strategic-initiatives/payments-security/scams/scamclassifier-model/.
[26] *See* CBA, et al., *supra* note 12.

groups provide an important service that could be disrupted by new data-sharing requirements, which can disproportionately harm vulnerable populations.

**Q18. 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 FraudClassifier℠ and ScamClassifier℠ models?**

The FRS, FDIC, and OCC can play a critical role in supporting further standardization of payments fraud data by building on the foundation provided by the FraudClassifier and ScamClassifier models. While these models represent an important first step in shaping the national conversation around fraud and scams, their effectiveness could be strengthened through structured engagement and increased acceptance. CBA members would support a comprehensive evaluation of both the adoption and deficiencies of the current models. This process should involve stakeholder groups that reflect a broad range of institutions and organizations of varying sizes and levels of maturity, as well as those that have and have not adopted the models to provide a comprehensive view of needs and challenges.

**Q19. 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 payments fraud data that would have the greatest impact on addressing fraud are those that improve client visibility across financial institutions. Information such as account age, transaction velocity (e.g., average number of checks written, history of returns, etc.), and history of prior charge-offs due to fraud. Additionally, data on activity occurring outside of financial institutions that impacts their customers. Consumers and businesses historically have been most impacted by check fraud, the rise in transaction limits and transaction speed has increased, driving significant increases in fraud occurring through P2P channels. When combined with criminals leveraging social engineering tactics to harvest and compromise data to facilitate fraudulent payments highlights the importance of sharing data on both transactions and the tactics criminals use to compromise accounts.

**Q20. 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, information sharing remains one of the key pillars for identifying and countering fraud and scams, and such a database would help facilitate those efforts. However, such a database is not without risk or challenge. For example, a data breach of such database could be catastrophic. Similarly, such a database may raise significant privacy concerns,

and questions over consumer consent and the ability to opt out of sharing their information in the database would need to be addressed. In recognition of the fact that consumers lead increasingly complicated financial lives, obtaining various financial products and services from banks and nonbanks alike, such a database should *not* be limited to information solely from large financial institutions, and instead should aggregate information about payments fraud across all market participants. Importantly, information sharing must extend *beyond* just the banking sector, as fraud and scams span multiple industries including social media, telecommunications sector, online platforms, and others. By expanding participation, the data will reflect the true cross-sector nature of fraud and scams. Ensuring that patterns can be identified quickly and stopped.

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

**Q21. 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?**

Risk management tools and services, operations, rules, and procedures should always be viewed through a lens that considers how malicious actors may access any publicly shared data and then leverage that data for nefarious purposes. For example, fraudsters have leveraged Paycheck Protection Program (PPP) information published by the Small Business Administration (SBA) to identify bank clients and commence impersonation scams.[27] These scammers would pretend to be representatives from the financial institution and trick PPP participants into sharing credentials or sending payments utilizing the information published by the SBA. While transparency and accountability are important for many of these programs, information that is reported out needs to be consistently examined for how the most sinister actors may seek to misuse it.

**Q22. 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?**

As a key operator of critical payment systems, the Federal Reserve plays an important role in not only ensuring system reliability, but also in advancing tools that help

[27] *See, e.g.*, Press Release, Nebraska Department of Banking and Finance, NDBF Issues Alert Regarding PPP Loan Scam (Jul. 10, 2025), *available at* https://ndbf.nebraska.gov/about/news-publications/ppp-loan-scam.

participants detect and prevent fraud. Private-sector networks, such as Mastercard and Visa, have built robust capabilities to monitor fraud across their rails; the Reserve Banks should follow these private-sector networks' example by expanding their own fraud mitigation services to better protect senders and receivers using Federal Reserve payment platforms.

The Reserve Banks are set apart by their distinct capability to identify patterns and risks at the network level across all financial institutions that utilize their services. Utilizing this unique capability, the Federal Reserve Bank should:

- Provide risk scoring tools based on transaction activity across the Federal Reserve-operated rails (FedACH, Fedwire, and FedNow), which would enable participants to better assess the fraud risk associated with sending or receiving parties;
- Implement mandatory or standardized fraud reporting mechanisms for transactions processed over Reserve Bank platforms, allowing for improved data aggregation, risk trend analysis, and targeted mitigation;
- Support the development and deployment of Confirmation of Payee services across payment types to help consumers and businesses verify recipient information before initiating payments, a proven tool in reducing authorized push payment scams in other markets; and
- Facilitate cross-rail fraud detection and insight sharing, particularly where fraud activity moves between systems, such as from ACH to FedNow.

## Payments Fraud Generally (Questions 23-26)

### Q23. 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?

While the specific impacts of payment fraud vary across institutions, certain trends have emerged as industry-wide concerns. Check fraud, impersonation scams, business email compromise, fraud involving digital payment channels, and both debit and credit card fraud have presented significant challenges. Criminals are employing increasingly sophisticated attacks on customers, many of which first originate outside of bank-managed channels, including endless phishing emails and spam texts.

Banks have long been at the forefront of protecting their customers against fraud and scams, but they cannot carry this fight alone, and the numbers reinforce this reality. According to new FTC data, reported losses to fraud jumped sharply in 2024, reaching 12.5 billion.[28] Particularly concerning is that many scams can be traced back to social media platforms, as highlighted in the recent Wall Street Journal article, Meta Platforms

[28] FTC, *supra* note 3, *available at* https://www.ftc.gov/news-events/news/press-releases/2025/03/new-ftc-data-show-big-jump-reported-losses-fraud-125-billion-2024.

"accounted for nearly half of all reported scams on Zelle for JPMorgan Chase between the summers of 2023 and 2024."[29]

In response, banks have taken extensive measures to protect customers across all payment channels. As noted in an Open Banker piece,[30] these measures include additional risk screenings, use of behavioral biometrics, digital ID verification, ongoing collaboration with law enforcement and many other safeguards designed to keep consumers and businesses safe from fraud and scams. This is also why there is an intrinsic benefit of credit cards as a payment vehicle. Interchange, the small percentage of a transaction merchants pay to the card-issuing bank, serves as a crucial component in the fight against fraud. A significant portion of these fees is used to fund the sophisticated fraud detection and prevention systems that protect both cardholders and financial institutions. These systems, often powered by AI, analyze transactions in real-time to identify suspicious activity, enabling card issuers to block fraudulent purchases and minimize financial losses. This is a vital function, especially considering the scale of the problem. For example, in 2024, the FTC received over 449,000 reports of credit card fraud, a number that continues to climb as fraudsters become more sophisticated.[31] Without the revenue from interchange fees, card issuers would struggle to maintain the advanced security measures that have enabled the widespread adoption and trust of digital payments.

**Q24. 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?**

CBA members have found leveraging fraud tools, such as positive pay to ensure that every customer's check will clear before being deposited, along with consortium data and vendor products to be useful in identifying, preventing, and mitigating payments fraud. Members have also utilized real-time alerts and client verification that incorporates behavioral analytics based on the client, as well as authentication controls. The transition to other payments rails that have increased protections, particularly the transition away from the use of checks, have enhanced protections. Consumers also play a vital role. Consumer education and awareness is important for identifying warning signs of scams that can help consumers avoid falling victim to scams. Moreover, informing institutions about incoming large payments or travel helps institutions know what activity is or is not fraud or scam connected, though consumers need to be

[29] Horwitz and Au-Yeung, supra note 14, *available at* https://www.wsj.com/tech/meta-fraud-facebook-instagram-813363c8?reflink=desktopwebshare_permalink.
[30] Brian Fritzsche, Banks Are Fighting Fraud and Scams, But We Can't Do It Alone, Open Banker (Jul. 10, 2025), *available at* https://openbanker.beehiiv.com/p/scamfighting.
[31] FTC, *supra* note 3, *available at* https://www.ftc.gov/news-events/news/press-releases/2025/03/new-ftc-data-show-big-jump-reported-losses-fraud-125-billion-2024.

cognizant that they are sharing this information with their depository institution in a safe and secure manner.

**Q25. To the extent not already addressed here, are there other actions that would support stakeholders in identifying, preventing, and mitigating payments fraud?**

CBA underscores that there needs to be an increased emphasis on participation from, and potential liability for failure to take meaningful steps to prevent fraud and scams by, technology, social media, and telecommunications industries. Additionally, it needs to be easier for consumers to report fraud and scams on these other industries' platforms. For example, when a consumer receives a text that is seeking to facilitate a scam, a consumer should have the option to click a button reporting the text as a fraud or scam, rather than just reporting the text as "junk."

Similarly, there needs to be a reevaluation of the treatment of vulnerable populations, particularly older adults, who face heightened risks of financial exploitation. As of January 2025, laws in about half the states allow banks to delay or deny transactions suspected of elder financial exploitation, with safe-harbor protections shielding institutions from litigation when acting in good faith to protect vulnerable customers.[32] For example, a Florida law authorizes financial institutions to "delay a withdrawal or transaction if bank employees suspect that a senior citizen or vulnerable adult is being financially exploited."[33] There is currently no federal counterpart to these protections though, leaving consumers in other states without similar safeguards. As the risk of scams targeting vulnerable populations continues to increase, such laws and safe harbors may need to be reconsidered at the federal level or in states that do not currently have such protections.

**Q26. Are there specific actions that commenters believe could encourage the use of payment methods with strong security features?**

N/A

* * *

CBA values the opportunity to comment on this RFI and appreciates the prudential regulators' exploration of ways to help counter the ever-growing threat of fraud and

[32] American Bankers Association Foundation, *State Hold Laws and Elder Financial Exploitation Prevention: A Survey Report* (Mar. 28, 2025), *available at* https://consumer.ftc.gov/system/files/consumer_ftc_gov/pdf/State%20Hold%20Laws%20and%20Elder%20Financial%20Exploitation%20Prevention%20(2025).pdf

[33] Al Pefley, New Florida law could protect seniors from getting scammed, CBS12, (Jun. 3, 2024), available at https://cbs12.com/news/local/new-fl-law-could-protect-seniors-from-getting-scammed.

scams. CBA is available to meet with the prudential regulators to discuss any of the issues identified in this letter and work together to develop tangible solutions.

Sincerely,

Brian Fritzsche
Vice President, Associate General Counsel
Consumer Bankers Association