FINANCIAL TECHNOLOGY ASSOCIATION, PENNY LEE

Proposal and Comment Information

Title: Request for Information on Potential Actions to Address Payments Fraud, OP-1866

Comment ID: FR-2025-0036-01-C71

Subject

FTA Comment Letter re Docket No. OP-1866 and RIN 3064-ZA49

Submitter Information

Organization Name: Financial Technology Association

Organization Type: Organization

Name: Penny Lee

Submitted Date: 09/18/2025

NONCONFIDENTIAL // EXTERNAL

Hello:

Please find attached the Financial Technology Association's response to the Federal Banking Agencies' Request for Information on Potential Actions To Address Payments Fraud. We appreciate your consideration of our comments and would be happy to discuss any of the items raised herein with you further.

Please don't hesitate to be in touch.

Respectfully submitted,
Angelena

Angelena Bradfield
Head of Policy
Financial Technology Association

FINANCIAL TECHNOLOGY ASSOCIATION

September 18, 2025

Chief Counsel's Office
Attn: Comment Processing
Office of the Comptroller
of the Currency
Suite 3E-218
400 7th Street SW
Washington, DC 20219

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

Ms. Jennifer M. Jones
Executive Secretary
Attn: Cmmts—RIN 3064-ZA49
Federal Deposit Insurance
Corporation
550 17th Street NW,
Washington, DC 20429

FTA Comment Letter re Request for Information on Potential Actions to Address Payments Fraud

(Docket ID OCC-2025-0009, Docket No. OP-1866, RIN 3064-ZA49**)**

The Financial Technology Association (FTA) appreciates the opportunity to respond to this Request for Information (RFI) from the Office of the Comptroller of the Currency (OCC), Board of Governors of the Federal Reserve System (FRB), and the Federal Deposit Insurance Corporation (FDIC) regarding potential actions to address payments fraud. We commend the agencies for taking proactive steps to solicit input from stakeholders across the country and recognize this as an important opportunity to promote secure, efficient, and innovative digital payments through public-private collaboration and smart policy design.

FTA is a nonprofit trade organization representing leading technology-centered financial services (fintech) companies. Our members are committed to advancing the responsible use of technology, which significantly improves the industry's ability to offer innovative financial products, including payment solutions, while maintaining robust compliance with regulatory standards.

As payments fraud evolves in scope and sophistication, so too must the policies and frameworks designed to prevent it. A growing share of fraud now occurs through noncard payments—such as checks, ACH, wires, and instant transfers—and these trends are particularly acute among small businesses and vulnerable populations.[1] The emergence of generative AI has introduced new fraud vectors, including AI-generated voice and identity impersonation schemes, that challenge traditional fraud prevention tools. As AI continues to evolve, it's essential for regulators and industry to adopt advanced detection tools and modern authentication techniques to address these risks effectively.

[1] *See* Federal Register (2025) *Request for Information on Potential Actions to Address Payments Fraud*, 89 FR 52186. Available at: https://www.federalregister.gov/documents/2025/06/20/2025-11280/request-for-information-on-potential-actions-to-address-payments-fraud.

Fortunately, fintech providers and payments firms are well-positioned to help combat these threats through innovative technologies and risk mitigation practices. However, doing so effectively requires modern policy frameworks and approaches, clear regulatory expectations, enhanced data sharing, and public-private collaboration.

FTA accordingly offers the following recommendations to improve the effectiveness and responsiveness of U.S. fraud prevention in the payments context:

1. **Modernize regulatory compliance and supervisory frameworks** to reflect evolving risks, including updates to BSA/AML program rules, CIP rules, CSI sharing, and improvements in public-private and private-to-private information sharing.

2. **Facilitate responsible development and adoption of advanced fraud detection tools,** including AI-driven solutions, by providing regulatory guidance and support for such adoption.

3. **Expand regulated access to core payment systems and modernize charter options** to improve regulatory visibility, reduce reliance on intermediaries, and strengthen fraud detection across the ecosystem.

4. **Promote a transition away from paper checks to secure, traceable digital payment solutions** to reduce fraud risk and improve payment security.

5. **Advance a coordinated national fraud strategy** grounded in law enforcement collaboration, including through establishing a federal and state digital fraud task force, and investing in financial awareness and education campaigns for high-risk groups.

I. The Federal Bank Agencies (FBA) Should Work to Modernize Compliance and Supervisory Frameworks to Bolster Fraud Prevention

Modernizing compliance and supervisory frameworks is foundational to any strategy aimed at reducing payments fraud. Outdated rules and regulatory expectations often limit the private sector's ability to detect and prevent fraud effectively, especially as criminals exploit faster payment systems, synthetic identities, and increasingly sophisticated tools such as generative AI. As detailed below, several key programs and rule sets require such modernization, necessitating joint agency efforts to harmonize expectations and ensure risk-based prioritization within financial programs.

A. The FBAs should reform BSA/AML requirements to focus on risk and outcomes and emphasize multi-stakeholder information-sharing

The current anti-money laundering and countering the financing of terrorism (AML/CFT) framework too often prioritizes process over impact. A "check-the-box" approach to compliance

can divert resources away from higher-risk activity and lead to defensive compliance measures, including an overwhelming volume of suspicious activity filings that are of limited value to law enforcement. The FBAs, working with FinCEN, should pursue a more risk-based approach that:

- Prioritizes high-value activity, enables resource allocation to higher-risk areas, and improves reporting outcomes through clearly expressed law enforcement priorities and feedback;[2]

- Trains examiners to understand and facilitate innovative AML/fraud technologies like behavioral analytics and real-time transaction monitoring, which can enhance compliance while reducing false positives; and

- Encourages flexible supervisory treatment and support for institutions that use these tools responsibly.

More specifically, payments fraud is increasingly fast-moving, cross-platform, and coordinated. Yet today's BSA/AML and information-sharing frameworks remain too fragmented, prescriptive, delayed, or limited to respond effectively. Financial institutions and their partners require better signals from law enforcement and greater ability to share relevant intelligence with one another and across the broader ecosystem more effectively.[3]

To strengthen information sharing and better align detection efforts with real-world risks, the FBAs should begin by grounding examiner expectations and AML program design in the National AML/CFT Priorities framework. By structuring risk-based AML programs around these priorities, firms would be able to focus compliance resources where they matter most.[4] Establishing structured feedback loops between law enforcement, FinCEN, and reporting institutions is essential to this effort. These loops should help identify and prioritize high-priority suspicious activity reports (SARs), reduce defensive or duplicative filings, and ensure BSA reporting is aligned with emerging fraud and illicit finance risks. Tools such as SAR "usefulness" indicators or law enforcement-issued priority flags could further help institutions calibrate their detection systems and improve reporting accuracy.

Agencies should also support the development of real-time information exchange mechanisms that enable institutions to share red flags quickly and efficiently across the industry. Fraudsters de-platformed by one institution can often continue operating elsewhere due to fragmented communication and delayed reporting. Agencies should promote efficient, real-time fraud alerting

[2] Financial Technology Association (2024a) *FTA Comment Letter re FinCEN's Anti-Money Laundering and Countering the Financing of Terrorism Programs Proposal*. Available at: https://www.ftassociation.org/wp-content/uploads/2024/09/FTA-AML-Program-Rule-Letter.pdf.

[3] Financial Technology Association, 2024a.

[4] Financial Technology Association, 2024a.

mechanisms that enable institutions to share red flags quickly and in structured formats, such as shared typologies, fraud indicators, or de-platforming signals.

In addition, the 314(b) safe harbor framework should be modernized to reflect the reality of today's payments and fraud landscape. The current framework is limited to sharing among financial institutions. It continues to raise questions around its scope, which can restrict the private sector's ability to act collectively against fraud schemes that cross traditional boundaries. Agencies should formally expand 314(b) eligibility to include fraud prevention networks, payments infrastructure providers, and other regulated service partners, and formally confirm in regulation that fraud-related information may be shared under the safe harbor. Updated guidance on permissible sharing scenarios would provide institutions with greater confidence and speed in coordinated responses.

Additionally, clarifying agency guidance around Reg CC and fraud-related fund holds in suspected fraud cases would also improve outcomes for both institutions and consumers. Today, institutions often provide limited or vague explanations to customers for account or payment holds to avoid violating SAR confidentiality rules or inadvertently "tipping off" a potential investigation. However, this approach can be counterproductive, as it may delay investigations or discourage customer cooperation. Agencies should consider clarifying how institutions can communicate transparently with customers about the nature of holds—without compromising SAR confidentiality—to improve fraud resolution, reduce friction, and enhance customer trust.

Finally, agencies should collaborate with FinCEN and encourage efforts to establish it as a central fraud intelligence hub. FinCEN should use its access to BSA data and law enforcement channels to issue real-time alerts, trend analysis, and priority risk typologies, especially for novel payment tools or emerging fraud vectors. These resources should be updated frequently, shared across the industry, and accessible to institutions of all sizes, including smaller banks and fintechs. Ensuring equitable access to actionable intelligence will help level the playing field for institutions serving high-risk or underserved communities and strengthen the industry's collective defense against fraud.

B. The FBAs should modernize the Customer Identification Program (CIP) Rule to reduce reliance on full SSNs and reflect digital, risk-based practices[5]

The existing CIP rule, adopted in 2003, does not reflect today's digital-first financial services environment or evolving consumer privacy expectations. We applaud the recent interagency and Federal Reserve exemption orders permitting, among other things, reliance on the last four digits

[5] Financial Technology Association (2024b) *Request for Information and Comment on Customer Identification Program Rule Taxpayer Identification Number Collection Requirement.* Available at: https://www.ftassociation.org/fta-calls-for-immediate-exceptive-relief-from-requirement-to-collect-full-nine-digit-ssns/.

of the SSN in appropriate circumstances. We encourage the agencies to continue modernizing the CIP rule to reflect technological advancements in identity verification.[6]

Regulators and modernized regulations should support secure, effective verification methods—such as multifactor authentication, behavioral analytics, and trusted third-party identity verification partners. Additionally, innovators are increasingly developing new approaches to identity verification that reduce privacy and security risks while increasing accuracy and effectiveness.[7] Updates to the CIP rule should accordingly contemplate not only legacy approaches to identity verification, but new technology-driven approaches that can improve compliance outcomes.

C. The FBAs should update and align Confidential Supervisory Information (CSI) sharing rules across agencies to enable sharing between banks and nonbank partners[8]

Modernizing CSI sharing policies is essential to improving fraud detection, facilitating timely remediation, and enabling more effective collaboration between banks and their fintech or nonbank service provider partners.

Current CSI sharing restrictions prevent banks from disclosing critical supervisory findings with partners, even when those partners are directly involved in operating or remediating compliance programs. This limitation creates unnecessary blind spots, slows down corrective action, and can increase fraud risk, particularly in complex or tech-enabled service delivery models.

Only the Federal Reserve currently permits limited CSI sharing with third-party service providers. The OCC and FDIC should adopt a similar approach, allowing banks to share CSI with fintech partners under strict and appropriate confidentiality protections. To enhance fraud prevention and risk management across the system, the FBAs should:

- **Issue joint guidance** clarifying permissible CSI sharing scenarios between banks and nonbank partners;

---

[6] Federal Deposit Insurance Corporation (2025) *Agencies Issue Exemption Order to Customer Identification Program Requirements.* Available at: https://www.fdic.gov/news/press-releases/2025/agencies-issue-exemption-order-customer-identification-program; Federal Reserve Board (2025) *Federal Reserve Board joins other federal financial institution regulatory agencies in providing banks the flexibility to use an alternative method for collecting certain customer identification information*. Available at: https://www.federalreserve.gov/newsevents/pressreleases/bcreg20250731a.htm.

[7] *See*, Persona (2025) *Faster verifications and less risk with Reusable Personas.* Available at: https://withpersona.com/blog/reusable-personas#:~:text=Introducing%20Reusable%20Personas:%20Persona's%20reusable,without%20sacrificing%20the%20user%20experience.

[8] Financial Technology Association (2024c) *Request for Information on Bank-Fintech Arrangements Involving Banking Products and Services Distributed to Consumers and Businesses.* Available at: https://www.ftassociation.org/wp-content/uploads/2024/10/FTA-Letter-on-Fintech-Bank-Arrangements-RFI.pdf.

- **Encourage timely and secure sharing** of supervisory findings to support faster remediation and reduce the need for abrupt program terminations that may harm consumers; and

- **Establish closed-loop communication channels,** such as agency-led advisory working groups or Bank Secrecy Act Advisory Group (BSAAG)-like structures, to enable collaborative discussion on emerging issues and strengthen supervisory transparency.

Aligning CSI-sharing policies across agencies will allow institutions and their partners to more effectively detect, respond to, and prevent fraud—without compromising regulatory integrity or confidentiality.

D. The FBAs should facilitate financial institutions—especially smaller banks—seeking to leverage leading third-party fraud detection tools and technologies

Payment fraud today is fast-moving, adaptive, and increasingly technology-driven, outpacing the capabilities of traditional compliance methods. The FBAs must evolve their oversight frameworks to actively support the widespread adoption of real-time, data-driven fraud tools across the financial ecosystem. This means providing clear guidance that encourages, rather than deters, banks from utilizing sophisticated third-party partners.

Smaller banks, in particular, face a unique challenge. Their smaller compliance teams and limited technology budgets often prevent them from developing cutting-edge fraud detection in-house. They are often the ideal candidates for partnering with fintech providers that specialize in advanced technologies such as behavioral analytics, real-time transaction monitoring, and automated identity verification.[9] However, current regulatory ambiguity can create a chilling effect, as these banks may fear that a reliance on third parties will be viewed as a compliance risk rather than a strategic strength. The FBAs should explicitly clarify that working with reputable technology partners and vendors to enhance fraud detection is not only permissible but is an expected component of a modern and effective risk management program.

Agencies should replace legacy compliance checklists with an oversight framework that prioritizes real-time responsiveness and outcomes. By providing consistent regulatory treatment, the FBAs can give smaller banks the confidence to embrace these partnerships, thereby enhancing fraud detection, reducing consumer harm, and strengthening the overall resilience of the financial system.[10]

[9] Financial Technology Association, 2024c.
[10] Financial Technology Association, 2024c.

E. The FBAs should develop a best practices playbook for fraud prevention and compliance

In line with the prior recommendation, the FBAs should move away from overly prescriptive, static rules and instead develop a dynamic, regularly updated playbook for fraud prevention. This approach, reflecting real-world innovations and evolving threats, would provide outcomes-oriented guidance and give banks the clarity and flexibility they need to combat modern financial crime. Instead of waiting for lagging regulatory actions, this playbook would serve as a proactive resource for institutions of all sizes.

The playbook should not be a rigid checklist but rather a framework that outlines best practices and principles. This could include:

- *Technology-Neutral Guidelines*: The playbook should focus on what a bank's fraud detection capabilities should achieve, rather than mandating specific technologies. This enables institutions to utilize advanced tools such as machine learning, behavioral analytics, and digital identity verification from third-party partners, without fear of regulatory pushback.
- *Emphasis on Third-Party Partnerships*: The playbook should explicitly encourage banks—especially smaller institutions with limited in-house resources—to leverage partnerships with specialized providers. This would provide clear guidance on due diligence, risk-sharing, and oversight, giving smaller banks the confidence to adopt sophisticated, real-time fraud tools.
- *Case Studies and Threat Intelligence*: The playbook should be a repository of anonymized case studies, best practices, and the latest threat intelligence. By sharing information on new fraud schemes and effective countermeasures, the FBAs can empower the entire financial ecosystem to stay ahead of bad actors.
- *A "Real-Time" Mentality*: The core of this approach would be a shift in focus from historical compliance audits to real-time detection and response. This would encourage banks to build systems that are responsive and adaptive, rather than simply checking boxes on a list. This outcomes-based framework would foster a culture of continuous improvement in fraud prevention.

II. The FBAs Can Take Key Steps to Facilitate Development and Adoption of Technologies to Combat Fraud and Financial Crime, Including through the Use of AI

The financial services industry continues to develop advanced technologies that significantly enhance fraud detection, risk monitoring, and regulatory compliance. These include artificial intelligence (AI), digital identity, and blockchain technologies. Among these innovations, regulatory technology (“regtech”) applications, in particular, can reduce compliance costs while

increasing the effectiveness of compliance programs, thereby strengthening trust in U.S. financial markets and services.[11]

Indeed, today, AI tools can be readily incorporated into a firm's transaction monitoring and fraud investigation processes to identify anomalous activity and accelerate the identification and resolution of complex fraud schemes. By analyzing large datasets, AI models can learn to distinguish legitimate transactions from increasingly sophisticated fraudulent activities, helping to identify potential fraud risks and prevent financial crime, often identifying risks that a human agent may overlook. The U.S. Department of the Treasury has already demonstrated the effectiveness of AI in fraud detection. In Fiscal Year 2023, the Treasury's Office of Payment Integrity used AI to help recover over $375 million by mitigating check fraud in near real-time.[12]

Despite these benefits, adoption of emerging technologies remains uneven, and regulatory clarity is often lacking. Regulators should promote responsible development and adoption of these tools by providing further guidance to the industry and, when appropriate for particular use cases, creating new pathways for piloting AI-based systems through sandboxes.

As a starting point, the FBAs should build on the 2018 joint statement from FinCEN, the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the National Credit Union Administration, and the Office of the Comptroller of the Currency, which encouraged financial institutions to adopt innovative approaches in their AML compliance programs. In that statement, the Agencies specifically underscored the important role of technology, noting that "[t]he Agencies recognize that private sector innovation, including new ways of using existing tools or adopting new technologies, can help banks identify and report money laundering, terrorist financing, and other illicit financial activity by enhancing the effectiveness and efficiency of banks' BSA/AML compliance programs."[13]

The FBAs should further clarify through guidance that many applications of AI—especially in the context of fraud and compliance—are not high-risk and therefore should be subject to properly calibrated risk management principles. Currently, ambiguity regarding whether certain AI applications are high-risk deters adoption of critical tools that could materially strengthen defenses, especially at smaller institutions, such as real-time fraud monitoring systems. While AI governance practices consistent with sound risk management principles are essential, they should be tailored to actual risks posed and subject to appropriate controls that do not preclude adoption in the first

[11] Financial Technology Association (2025a) *Request for Information on the Development of an Artificial Intelligence (AI) Action Plan.* Available at: https://www.ftassociation.org/wp-content/uploads/2025/03/FTA-Letter-on-the-Development-of-an-AI-Action-Plan-RFI.pdf.

[12] U.S. Department of the Treasury (2024) *Treasury Announces Enhanced Fraud Detection Process Using AI Recovers $375M in Fiscal Year 2023.* Available at: https://home.treasury.gov/news/press-releases/jy2134.

[13] U.S. Department of the Treasury (2018) *Treasury's FinCEN and federal banking agencies issue joint statement encouraging innovative industry approaches to AML compliance*. Available at: https://home.treasury.gov/news/press-releases/sm562.

place. We detail more on risk management guidance and ways for regulators to spur responsible adoption of AI in *FTA's 2025 AI Action Plan* comment letter.[14]

Beyond regulatory guidance and regulator support for compliance technologies, it is further critical that financial institutions, payments providers and entities that support the fraud detection and prevention ecosystem have access to high-quality data used to train and validate AI tools. Regulators should accordingly support partnerships to build shared fraud datasets, develop model benchmarks, and promote transparency, potentially through BSAAG subcommittees (in coordination with FinCEN) or new interagency working groups. To this end, we encourage the FBAs to provide technical assistance to the CFPB as it reopens the Section 1033 open banking rule to ensure that an amended rule removes restrictions on the secondary use of permissioned data, which may unnecessarily limit access to data that can assist the development of more effective and accurate fraud models. Finally, the government should seek opportunities to provide financial institutions and their fraud detection and prevention partners with access to high-quality government-held datasets that can be used to train new models.[15]

III. The FBAs Can Help Counter Fraud by Expanding Access to Payment Systems and Modernizing Banking Charters

Granting a broader set of well-regulated fintechs and payment firms with direct access to national payment systems is a crucial step in combating fraud and financial crime. By enabling more direct participation, regulators can gain increased transparency into payment flows and establish more direct communication channels with providers.

A modernized and proactive regulatory approach should focus on facilitating this access and fostering a more diverse and resilient ecosystem. Regulators can achieve this by championing a range of chartering and licensing options. This includes supporting the development of optional federal payments charters, continuing to expand approvals for so-called Tier 3 banks, and encouraging de novo charters, including ILCs. These approaches would bring more providers under direct oversight while enabling safe, supervised participation in key infrastructure. Doing so would improve data transparency, reduce reliance on unnecessary intermediaries, and increase regulators' line of sight into end-to-end payment flows.[16] This strategy not only modernizes banking and payments but also creates a more robust and fraud-resilient financial system for all.

Additionally, participation in FedNow and other core payment systems should be available to a broader set of qualified, regulated entities. Fintechs and payment companies that meet appropriate risk management, supervisory, and operational standards should be permitted to participate

[14] Financial Technology Association, 2025a.
[15] Financial Technology Association, 2025a.
[16] Financial Technology Association, 2025b.

directly in these systems, thereby improving access to faster, traceable, and fraud-resilient payment systems. Treasury's own adoption of FedNow for public disbursements demonstrates the value and feasibility of broadening access to modern payment rails.[17]

IV. The FBAs Should Promote a Transition from Paper Checks to Secure Digital Payments

Paper checks remain one of the most fraud-prone and least secure payment methods in widespread use today. While other payment systems have evolved to include built-in traceability, real-time monitoring, and authentication safeguards, physical checks have remained vulnerable to theft, forgery, and alteration. Check fraud incidents doubled between 2021 and 2022, and checks are over 16 times more likely to be lost, stolen, or altered than other payment types.[18]

Unlike digital payments, checks offer limited visibility into transaction status and minimal protection against interception or manipulation once mailed or deposited. This lack of transparency creates challenges for consumers and financial institutions alike and weakens efforts to detect and prevent fraud in real-time.

In contrast, digital payments—especially those processed through real-time systems—enable enhanced monitoring, automated red-flag detection, and faster resolution when fraud is suspected. A coordinated transition away from paper checks toward secure, traceable digital payments would reduce fraud risk, improve payment speed, and enhance consumer protections, while aligning regulatory frameworks with modern payment practices. Broader use of regulated digital wallets, fintech-enabled bank accounts, and prepaid digital tools can expand access to safer financial services.

Following the U.S. Treasury Department's recent request for comment regarding combatting fraud, and to support this transition to digital payment solutions, the FBAs should work with Treasury to invest in public awareness and education campaigns. Public awareness efforts should help consumers understand the risks associated with paper checks and the benefits of modern digital tools, especially in high-risk and underserved communities. We provide more detail on potential education and awareness campaigns in our recent Treasury comment letter.[19]

---

[17] Financial Technology Association (2025b) *FTA Comment on Request for Information Related to E.O. 14247 – Modernizing Payments To and From America's Bank Account*. Available at: https://www.ftassociation.org/wp-content/uploads/2025/07/FTA-Letter-re-Treasury-RFI-on-Modernizing-Payments-under-EO-14247.pdf.

[18] Financial Technology Association, 2025b.

[19] Financial Technology Association, 2025b.

V. The FBAs Should Promote a National Fraud Strategy Underpinned by Law Enforcement and Public Education

Payments fraud is a national challenge that requires a coordinated, public-private, and cross-sector response. A comprehensive national fraud strategy, underpinned by law enforcement coordination, unified reporting, and targeted public education, would help disrupt fraud networks, better equip high-risk communities, and restore consumer trust in modern financial services.

Federal and state law enforcement agencies should strengthen collaboration to investigate and dismantle fraud networks, including through the creation of a joint federal-state digital fraud task force. We support efforts like the *Task Force for Recognizing and Averting Payment Scams Act* to assist in coordinating public and private sector efforts to combat scams. We believe it is important to have broad industry representation in such initiatives, given the speed and sophistication of scams. Many of today's fraud schemes are transnational, tech-enabled, and fast-moving, making traditional investigative models too slow or fragmented to be effective. Law enforcement should also work directly with telecommunications providers, web hosts, search engines and social media platforms to reduce the volume of scam texts, spoofed caller IDs, and fraudulent online content, which remain major vectors for fraud. Regulators should redouble efforts to coordinate with these industries as part of a comprehensive fraud strategy and call for investment into law enforcement strategies.

In parallel, the government should collaborate with industry to modernize fraud reporting to streamline data collection and reduce duplication. Today, fraud reports are scattered across multiple portals that exist across agencies and sectors, often with overlapping or inconsistent information. Due to the evolving nature of fraud, the reporting frameworks can also quickly become outdated, requiring filers to retrofit the activity into a certain fraud classification scheme. This fragmentation not only increases the burden on institutions and consumers, but also reduces the utility of the data for trend analysis and enforcement. A centralized reporting hub that keeps pace with evolving fraud typologies would improve data accuracy and completeness, enable faster investigations, and enhance transparency for both the public and private sectors.

Education should also play a central role in any national fraud strategy. As noted above, public awareness campaigns should equip individuals, especially those in high-risk groups, to understand how to identify and avoid fraud, and how to access secure digital financial services. These efforts should focus on underserved groups, including older adults, small businesses, and unbanked or underbanked individuals, and be delivered in accessible, multilingual formats through direct engagement with trusted community channels.[20]

[20] Financial Technology Association, 2025b.

Agencies should also update consumer-facing educational resources—including the FDIC's "Get Banked" campaign—to reflect modern financial tools such as regulated digital accounts, fintech-enabled bank products, and other modern, secure alternatives. And as fraud evolves, so too should law enforcement training. Agencies should invest in education for law enforcement officers on how fraud occurs, the technologies being used to detect and fight it, and the tools that bad actors are now leveraging—including AI-driven scams and identity theft.

***

We appreciate the opportunity to contribute to this discussion and support the government's efforts to mitigate payments fraud. FTA and its members stand ready to partner with the agencies and other stakeholders to advance effective, innovation-compatible solutions that protect consumers and strengthen the U.S. payments system.

Sincerely,

Penny Lee
President and Chief Executive Officer
Financial Technology Association