September 18, 2025

Via Electronic Delivery

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

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

Jennifer M. Jones
Deputy Executive Secretary
Attention: Comments-RIN 3064-ZA49
Federal Deposit Insurance Corporation
550 17th Street NW
Washington, DC 20429

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:

Capital One Financial Corporation ("Capital One")[1] greatly appreciates the opportunity to comment on the *Request for Information on Potential Actions to Address Payments Fraud* (the RFI).[2] We share your commitment to defending the public from criminal actors, including the threat of increasingly sophisticated scammers targeting consumers, businesses, and organizations spanning all sectors of the U.S. economy and society. Thank you for the opportunity to share our perspective on this important matter and to provide more information on Capital One's approach to keeping customers safe, through our continuous investment in the industry-leading tools, technologies, and analytics needed to fight international criminal scams and fraud.

---

[1] Capital One Financial Corporation (www.capitalone.com) is a financial holding company which, along with its subsidiaries, had $468.1 billion in deposits and $659.0 billion in total assets as of June 30, 2025. Headquartered in McLean, Virginia, Capital One offers a broad spectrum of financial products and services to consumers, small businesses and commercial clients through a variety of channels. Capital One, N.A. has branches and Cafés located primarily in New York, Louisiana, Texas, Maryland, Virginia and the District of Columbia. A Fortune 500 company, Capital One trades on the New York Stock Exchange under the symbol "COF" and is included in the S&P 100 index.

[2] Office of the Comptroller of the Currency, Treasury; Board of Governors of the Federal Reserve System; and Federal Deposit Insurance Corporation, Request for Information on Potential Actions to Address Payments Fraud, 90 Fed. Reg. 26293 (June 18, 2025), available at https://www.federalregister.gov/documents/2025/06/20/2025-11280/request-for-information-on-potential-actions-to-address-payments-fraud.

Capital One supports efforts that advance common-sense, pragmatic strategies that get to the root of these global problems. As the threat environment evolves — and as the malicious actors driving these crimes become more innovative, determined, and well-resourced — one thing has become abundantly clear: no single institution or industry can unilaterally solve this problem. Financial institutions continuously invest in modernizing the payments ecosystem to combat fraud and scams, but to effectively address the expansive issue at hand we must take a global, multi-faceted approach that reaches well beyond financial institutions alone.

In the material that follows, we outline our perspective on the evolution and trajectory of financial scams and fraud and share recommendations for action that can be taken to meaningfully strengthen protections for all Americans. This includes recognition of the vital role your organizations play in confronting the crisis of financial scams. Thank you again for your leadership on this front and for the opportunity to provide our perspective.

Our Focus on Combatting Criminal Scams and Fraud

Capital One is unique amongst large banks in that we were created and built in the last few decades. That relatively new position in the market is reflected in the differentiated approach we take to designing our products and serving our customers. When it comes to ensuring the financial health and wellbeing of our customers, we put innovation and consumer-first policies front and center. A critical part of that is our work to continuously invest in the enhanced technologies and layered defenses needed to prevent consumers from being victimized by criminals. These efforts include customer education campaigns, coordination with law enforcement, and real-time transaction monitoring and intervention. Importantly, and in parallel to these protections, we provide zero liability for unauthorized transactions in a policy that goes above and beyond what is required under federal law.

We also recognize that protecting consumers from criminal fraud and scams requires better information and partnerships for addressing the broader threat landscape. That was the impetus behind our decision to join the Aspen Institute's National Task Force for Fraud & Scam Prevention, an effort launched last year to galvanize action and information sharing across industry, government, and law enforcement. Capital One has also partnered with the Better Business Bureau (BBB) Institute for Marketplace Trust on critical consumer education campaigns, including the launch of the BBB Scam Tracker to help consumers better identify and report scams. In partnership with the BBB and Amazon, we introduced the Scam Survivor Toolkit to provide personalized recovery plans to scam survivors. Capital One also has a longstanding partnership with the education nonprofit Khan Academy, focused on helping individuals become financially empowered through a free online financial literacy course. Since the beginning of our partnership in 2023, approximately 2.1 million users have spent 65.5 million minutes learning about financial literacy in this course. Last year, we set a world record[3] with this course for the most users to take a financial literacy course online in 24 hours.

Taken together, these actions reflect our unwavering commitment to protecting consumers from financial crimes and our relentless drive to identify and thwart the bad actors from across the globe who seek to exploit them. But as the criminals perpetrating these attacks become increasingly more sophisticated, we know we can't do it alone. To keep pace with the increasing resourcefulness and determination that defines this threat, new solutions and partnerships are needed, especially at a time when more of these crimes are originating overseas within global crime syndicates.

[3] "Capital One Sets a World Record," October 16, 2024, https://www.capitalone.com/about/newsroom/capital-one-sets-a-guinness-world-record/

Distinguishing between scams and fraud

The RFI covers both “payments fraud” and “scams,” defining scams as a subset of fraud. But scams are a fundamentally different problem that require a fundamentally different policy solution. It is important to distinguish between fraud and scams and to treat them as separate issues when analyzing policy options. The Electronic Fund Transfer Act (EFTA) illustrates why.

The U.S. government has an important tool at its disposal in EFTA and Regulation E (Reg E) which implements EFTA. Congress enacted EFTA to safeguard consumers, incorporating within its text the dynamic of shared responsibility across banks, payors, and payees to help manage and mitigate fraud and scams. The primary purpose of EFTA is to protect consumers from liability for transactions they did not authorize. As you are aware, the law draws a distinction between fraud and scams. Fraud involves an unauthorized transaction, where a criminal gains access to a customer's bank account and initiates a payment without their consent.

EFTA ensures bank liability for fraudulent transactions outside of the customers’ control. However, the policy does not apply in cases where a customer has willingly made a transaction of their own volition. An example of this is when a customer has been tricked or manipulated into transferring funds to a criminal actor. In these instances, banks typically have little to no visibility into the customer’s interactions with the criminal, making it hard, if not impossible, for the bank to intercede. Even when banks do manage to spot these threats and attempt to intercede, the customer is often so convinced by the scammer’s lies that they continue with the transaction anyway, seeking alternative payment rails to complete the transfer.

External Collaboration, Data Collection, and Information Sharing

Combatting fraud and scams requires shared responsibility and collaboration across the ecosystem. The threat of bad actors seeking to exploit and steal from American consumers is not confined to a single platform or payment type. Every day, criminals from around the globe seek to impersonate agents of federal and state governments, law enforcement officials, and the critical welfare agencies that Americans rely on to meet their daily needs.[4] Beyond these tactics, well-funded criminal organizations also now have the capabilities to perpetuate elaborate investment and romance scams, sell non-existent goods and services, and even impersonate loved ones by leveraging technology including but not limited to Artificial Intelligence (AI). While this rapidly evolving technology is becoming increasingly available to the public, criminals are investing significant resources to be able to use AI in their sophisticated programs to scam customers. These AI tools — particularly deepfake technologies that make it easier for criminals to impersonate the voice and likeness of trusted individuals — will only serve to enhance the believability of these scams.

These anecdotes are borne out in the data, which show scammers have shifted from hacking financial systems to hacking individuals and manipulating them into their own financial exploitation. As the minority staff for the Joint Economic Committee (JEC) recently reported, “[d]igital scam losses have increased 370% in the U.S. over the past five years, and scam victims lost $1 trillion last year

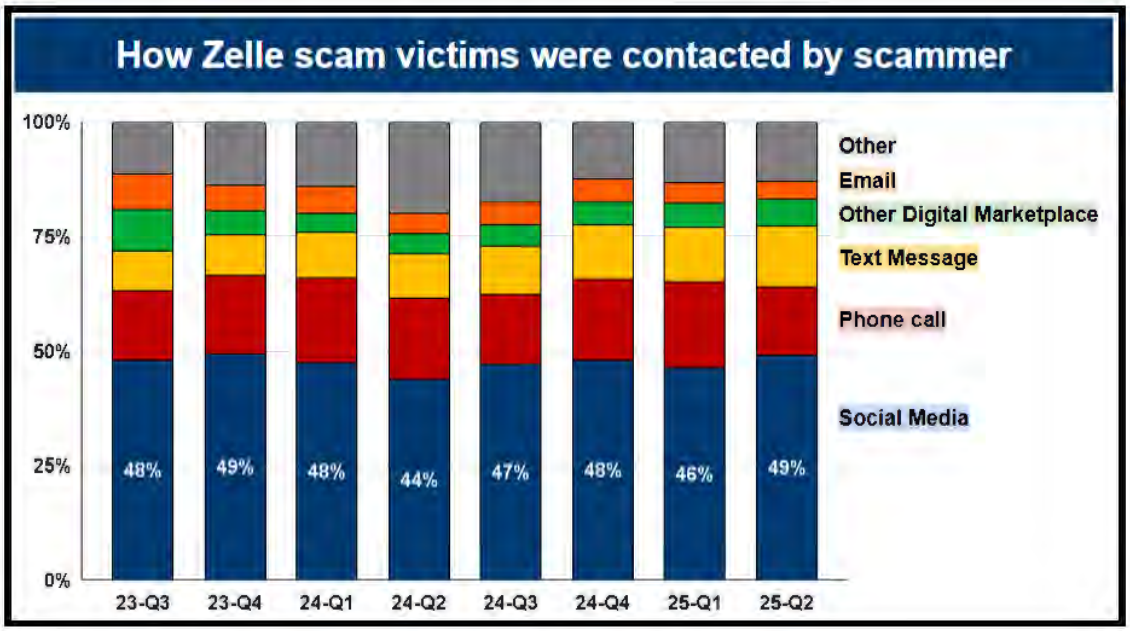
[4] "How to Avoid Imposter Scams," Federal Trade Commission, last modified July 2019, https://consumer.ftc.gov/features/how-avoid-imposter-scams.

globally."[5] Notably, financial institutions are just one part of an expansive, multi-sector ecosystem that criminals seek to exploit. By the time consumers reach the final step of providing the money in a scam transaction, a vast and elaborate system of deception has already taken place—one that, in more and more cases, may originate with an overseas crime ring,[6] and that has almost certainly travelled across multiple channels and networks, from spoofed phone calls and text messages to fake ads on social media platforms. While criminals historically have targeted older Americans, they are broadening their scope and targeting Americans of all demographics who do not necessarily see themselves as susceptible to fraud and scams.[7]

Banks are just one part of a vast ecosystem impacted by criminal fraud and scams. And we believe protecting consumers from the perpetrators of these crimes requires a whole-of-society approach. To truly safeguard Americans and combat malicious actors, we must have a coordinated effort across public and private entities that spans across industries. This means bringing the telecommunications industry, social media platforms, national security officials, law enforcement, and the entire financial services sector to the table to advance solutions in partnership.

Collaboration and information sharing with social media companies

We believe meaningful progress can be made to combat fraud and scams that originate with social media companies. Based on what our customers have shared with us during our claims intake process, we estimate that approximately 45% of all Zelle scam transactions originated via social media contact.



[5] "July 2025 Issue Brief: Scams," Joint Economic Committee, U.S. Senate, July 2025, https://www.jec.senate.gov/public/_cache/files/d229cc6d-0dc5-4828-9f92-5de8ffffa326/july-2025-issue-brief-scams-1.pdf.
[6] "The Vast and Sophisticated Global Enterprise That Is Scam Inc.," *The Economist*, February 6, 2025, https://www.economist.com/leaders/2025/02/06/the-vast-and-sophisticated-global-enterprise-that-is-scam-inc.
[7] "$50,000 in a Shoe Box and Handed It to a Stranger I never thought I was the kind of person to fall for a scam," *The Cut*, February 15, 2024. https://www.thecut.com/article/amazon-scam-call-ftc-arrest-warrants.html

We have seen a wide array of tactics that criminals deploy both on and off social media platforms, including advertisements for fake goods and services[8] to steal payment credentials and money, and building relationships with vulnerable victims, emotionally manipulating them into sending financial resources through romance scams. As scams broaden in their sophistication, Americans of all demographics are being more heavily impacted, although senior citizens are particularly vulnerable. According to the FBI's annual internet crime report, Americans over the age of 60 suffered the most losses, reporting nearly $5 billion, which is a 43% increase over the previous year. Further, seniors submitted the greatest number of fraud and scam-related complaints compared to other groups. When it comes to romance and confidence-based scams such as "pig butchering", no demographic group is immune to this tactic, but an increasing number of seniors are being victimized by these complex schemes.[9] Additionally, a recent Federal Trade Commission (FTC) report[10] found criminals are increasingly targeting older Americans and stealing their life savings by pretending to be trusted businesses and government agencies. Addressing scams that originate on social media will require stronger obligations for social media companies to take scams seriously.

We endorse the potential recommendations for social media companies to strengthen policies and procedures to combat financial crime. The following suggestions are reflected in responses from our industry trade partners including, but not limited to, efforts such as:

- Report confirmed scam activity to a national registry and law enforcement in a timely manner.
- Develop standardized, cross-platform consumer reporting mechanisms.
- Standardize reporting and intelligence-sharing processes with financial institutions to protect shared customers.
- Create a standardized, cross-platform reporting mechanism to allow consumers to report scam activity that appears across multiple social platforms.

Collaboration with telecommunications providers

Our work with telecom providers to prevent spoofing of Capital One phone numbers is an illustration of what is possible when industries work together to prevent scams. It also highlights the gaps and limitations that still exist. Caller ID spoofing has been a persistent and pernicious attack vector over time. Bad actors are able to manipulate the information that appears on phone screens when they call their potential victims, making it appear as though they are calling from their target's bank, often under the pretense of protecting them from fraud or scams. 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 transaction, or mail a debit card.

Up until the past year, there was no way to protect our own Capital One 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 the

[8] "Meta battles 'epidemic of scams' as criminals flood Instagram, Facebook," *The Wall Street Journal*, May 17, 2025, https://www.wsj.com/tech/meta-fraud-facebook-instagram-813363c8.
[9] Federal Bureau of Investigation. *2024 Internet Crime Report*. Internet Crime Complaint Center. https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf
[10] "False alarm, real scam: how scammers are stealing older adults' life savings," The Federal Trade Commission. August 7, 2025. https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2025/08/false-alarm-real-scam-how-scammers-are-stealing-older-adults-life-savings

problem. We now use this new service to protect Capital One-owned phone numbers from being spoofed by bad actors. As a result, we have blocked more than *five million* spoofing attempts against our toll free numbers, branch numbers, and cafe numbers. While we are encouraged by the progress in our own ability to block these attempts, we also recognize the limitations of these developments. For one, we are only able to protect our own phone numbers and can only do so for phone calls. There is currently no way to prevent spoofing of text messages, nor is there a clear path for bringing the bad actors using spoofed phone numbers or text messages to justice.

Addressing scams that originate with telecommunications providers will require stronger obligations for companies to take scams seriously. We endorse the potential recommendations reflected in responses from our industry trade partners including, but not limited to, efforts such as:

- Enforce anti-fraud standards consistently across Mobile Virtual Network Operators (MVNOs).
- Adopt stronger Know-Your-Customer controls to prevent criminals from using telecom accounts to disseminate scams.
- Establish scam reporting and prevention methodologies similar to those that allow consumers to report and prevent spam communications.
- Ensure major carriers enforce anti-fraud standards for mobile virtual network operators that lease their networks.
- Create 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.

Collaboration and information sharing across the world

It is important to note the alarming trends with respect to how globally networked the perpetrators of these crimes have become. A recent series of reports from *The Economist* [11] sheds light on the vast network of underground scam syndicates now operating in Southeast Asia, Africa, Eastern Europe, the Middle East, and South America. 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.[12]

In addition, we can learn from successful domestic and international data sharing models, such as Australia's National Anti-Scam Centre to expand data sharing with targeted goals and aligned incentives / obligations for participants to provide data.

Collaboration across and with law enforcement agencies

We believe that law enforcement agencies must play a central role in prosecuting criminality, deterring future bad actors, and protecting consumers. Capital One is committed to partnering with law enforcement on all levels – state, local and federal. Our goal is to coordinate and build strong relationships with law enforcement agencies to help combat financial crimes and assist law enforcement with their investigations. While we have a wide range of external partnerships, each with their own unique role in combatting fraud and scams, we see the need for more collaboration from

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

other industries to help more effectively fight criminals and bring justice to victims. We are proud to be part of the Advisory Board of the North America Chapter and Global Advisory Board of the Global Anti-Scam Alliance (GASA). GASA brings together key industry stakeholders to share knowledge and best practices while fostering collaboration to protect consumers and fight financial crimes across the globe. Forums such as GASA can help bring to life collaborative ideas to empower law enforcement in fighting crime. Efforts to arm law enforcement agencies with more centralized tools for tracking scams and fraud and for sharing information could go a long way in making it easier to identify prevalent activity and large crime rings.

Fighting financial crime requires collaboration across industries – social media, telecommunications, finance, technology, law enforcement, and government at every level. To most effectively combat the increasingly sophisticated and well-funded criminals who carry out fraud and scams, we need to come together to create and scale a multidisciplinary and comprehensive whole-of-society approach. We are encouraged by our partnerships across sectors to take on financial criminals, yet still see the need for greater collaboration. The federal government is uniquely positioned to serve as a convener that can bring together key stakeholders to bolster collaboration, foster innovation, and work towards ensuring the safety and security of the American people. Capital One stands ready to partner across sectors to combat crime.

Consumer, Business, and Industry Education

Education is critical to combatting fraud and scams. To start- and as noted earlier in this letter- the law makes clear the distinction between fraud and scams. Understanding the difference between the two is critically important for consumers, as these terms are often used interchangeably, despite their significant differences. The U.S. government, as an influential and well respected convener, has the opportunity to continue educating Americans about the differences within financial crimes including fraud and scams. With respect to scams, the government has a distinct role to play. This includes not only educating individuals and businesses on how to spot scams, but also industry, law enforcement, and government on how to defend against them. These education efforts already exist, but they are often overlapping, incomplete, or simply too small. A whole-of-society approach to combatting criminal fraud and scams would ideally include a centralized education plan. The executive branch is in the best position to lead a centralized plan to educate individuals across all levels of government, industry, and individuals.

To keep pace with the increasing resourcefulness and determination that defines this threat, new solutions and partnerships are needed, especially at a time when more of these crimes are originating overseas within global crime syndicates. Private action is not enough. We encourage efforts from the government to develop a centralized plan that would educate the public, other government entities, and the industry about scams and fraud and tools that are available to combat them. For example, the plan could cover areas such as:

- Consumer education: familiarize consumers with tools they can use to identify scams and fraud more quickly, such as specialty consumer reporting agencies and encourage consumers to keep track of bank accounts that may be reporting against their consumer profile, which aren't visible in general consumer credit reports and credit bureau alerts.
- Government education: educate federal, state, and local law enforcement about fraud and scams trends and resources that are available to help prosecute bad actors and recover money for victims. Financial crimes are global in scale, but combatting them requires local efforts.

- Industry education: develop more resources that industry can use to understand the latest trends so that industry can better track and fight fraud and scams.

Regulation and Supervision

As criminals continue to ramp up their efforts to take advantage of and steal from consumers, we need to collectively do more to ensure all stakeholders have the tools necessary to combat financial crime. This includes, but is not limited to considering modifications to existing regulations and supervisory mechanisms to further bolster our efforts.

In our view, the current regulatory framework generally apportions responsibilities and liabilities appropriately. For example:

- The liability framework in EFTA and the Truth in Lending Act appropriately shifts liability to banks where banks are in the best position to mitigate fraud, but does not shift liability to banks for activities that are beyond their control. See above for more discussion on EFTA's purpose and liability provisions.
- The Gramm-Leach-Bliley Act imposes privacy restrictions, but it allows banks to share nonpublic information "to protect against or prevent actual or potential fraud, unauthorized transactions, claims, or other liability."[13]

Because criminals are constantly developing new techniques, banks must be able to innovate and implement creative solutions to combat it. Increasing regulatory or supervisory actions could hinder those efforts to innovate and negatively impact consumers. Also needing to comply with a patchwork of inconsistent laws and regulations can also hamper efforts.

Capital One urges the agencies to work collaboratively with the banking industry to streamline supervisory practices and modernize key regulatory definitions and authorities. Doing so will better equip financial institutions to address both existing and emerging threats specific to both fraud and scams—and to protect the consumers and systems most at risk. These are areas that would provide the greatest benefit.

Modernize ACH and Check Frameworks to Mitigate Abuse

Capital One would support legislative actions that would incentivize financial institutions to partner to mitigate the risk of payments fraud in ACH space. NACHA operating guidelines are not equipped to mitigate abuse of the ACH framework.

For example, a common fraud technique is where fraudsters establish a legitimate ACH link in their own name, complete a pull payment with an Originating Depository Financial Institution (ODFI) and then submit a claim of fraud to the Receiving Depository Financial Institution (RDFI). Under existing NACHA operating guidelines, the ODFI has no recourse to contest the claim; the funds are automatically sent back to the fraudster's account. Capital One supports continued investment in the modernization of the ACH system to ensure it remains well suited to manage critical risks.

Capital One would also support actions that would move the industry to more secure and modern payment methods, which can help phase out checks. While allowing for more flexibility under

[13] GLBA sec. 502(e); 12 C.F.R. 1016.15.

Regulation CC would help to implement better fraud guardrails, changes to Regulation CC are a lower priority than investing in the future state of payments.

Support common sense bipartisan legislation in Congress

We believe Congress has the opportunity to advance bipartisan solutions to create a safer financial ecosystem for all Americans. We were one of the first financial institutions to endorse bipartisan legislation that advances common sense, pragmatic strategies that get to the root of these global problems. Specifically, we hope that Congress will advance legislation to create a crucial public-private task force this session. The "Task Force for Recognizing and Averting Payments Scams (TRAPS) Act[14]," would establish such a task force to formally coordinate efforts, develop best practices, and recommend comprehensive solutions. Currently, the response to payment scams is fragmented. Government agencies, financial institutions, telecom and social media companies often work in silos. Congress has the opportunity to create a coordinated mechanism whereby all players can share intelligence, develop best practices, and create a unified defense against increasingly sophisticated scammers. The TRAPS Act would create such a formal structure for collaboration to make the entire financial ecosystem safer for consumers. We appreciate the efforts of Senators Mike Crapo (R-ID), Mark Warner (D-VA), Jerry Moran (R-KS), Raphael Warnock (D-GA) and Bill Cassidy (R-LA) to advance this bill.

In the House, the "Guarding Unprotected Aging Retirees from Deception (GUARD) Act"[15] would allow state and local law enforcement to use eligible federal grant funding to investigate financial fraud and scams against retirees. It also requires the Treasury Secretary and the Director of the Financial Crimes Enforcement Network (FinCEN) in consultation with the Attorney General, the Secretary of Homeland Security, and the appropriate Federal banking agencies and functional regulators to submit to Congress a report on efforts and recommendations to combat such scams. We applaud Representatives Zach Nunn (R-IA), Josh Gottheimer (D-NJ), and Scott Fitzgerald (R-WI) for their work to bring attention and solutions to these issues.

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.

Reserve Banks' Operator Tools and Services

We agree with our industry trade partners that the Federal Reserve plays an important role in not only ensuring system reliability, but also in advancing tools that help participants detect and prevent fraud in its role as a key operator of critical payment systems. In that role, the Reserve Banks should continue expanding their own fraud mitigation services to better protect senders and receivers using Federal Reserve payment platforms.

We endorse the potential recommendations reflected in responses from our industry trade partners including that the Reserve Banks are uniquely positioned to identify patterns and risks at the network

[14] 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 June 10, 2025, https://www.congress.gov/bill/119th-congress/senate-bill/2019.
[15] H.R. 2978, "Guarding Unprotected Aging Retirees from Deception Act" or "GUARD Act," 119th Cong. (2025), introduced April 21, 2025, https://www.congress.gov/bill/119th-congress/house-bill/2978.

level—across all financial institutions using their services—and should build tools that leverage that visibility. We would also prioritize recommendations to:

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

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

***

In closing, Capital One remains a deeply committed partner in combating sophisticated financial criminals and looks forward to collaborating with our peers across industries to ensure the safety of the public. A number of common sense solutions have been proposed by a range of banking trade associations that we believe could meaningfully address the root of the challenge, and which we would be happy to discuss with you. We appreciate the opportunity to comment on these important issues, and welcome the opportunity to discuss our recommendations further at your convenience. Please let us know if you have further questions.

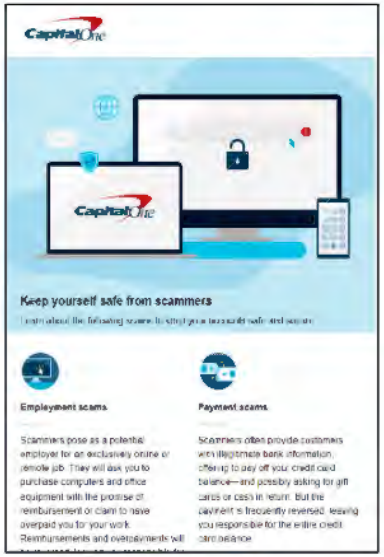
Sincerely,

Andres L. Navarrete
Executive Vice President
Global Enterprise Affairs

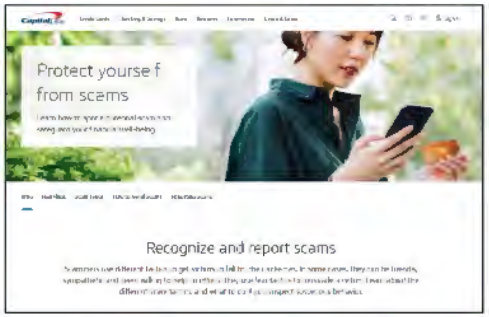
We proactively educate customers about scams across our channels

Customer Education

Quarterly Emails

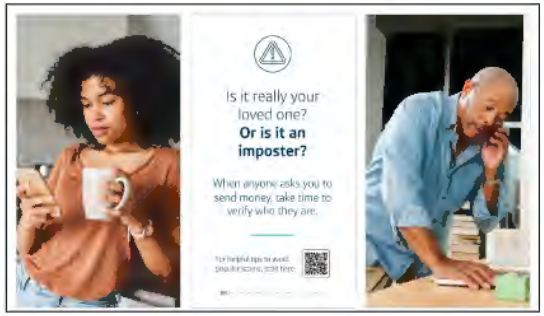


Scam Education Website



https://www.capitalone.com/digital/scam-education/

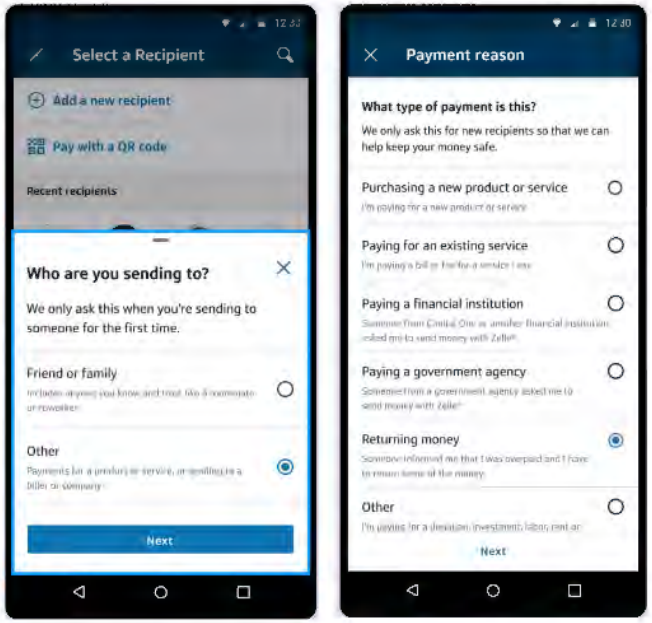
Physical Signage



Choose a Send Reason offers payment scenario based scam messaging

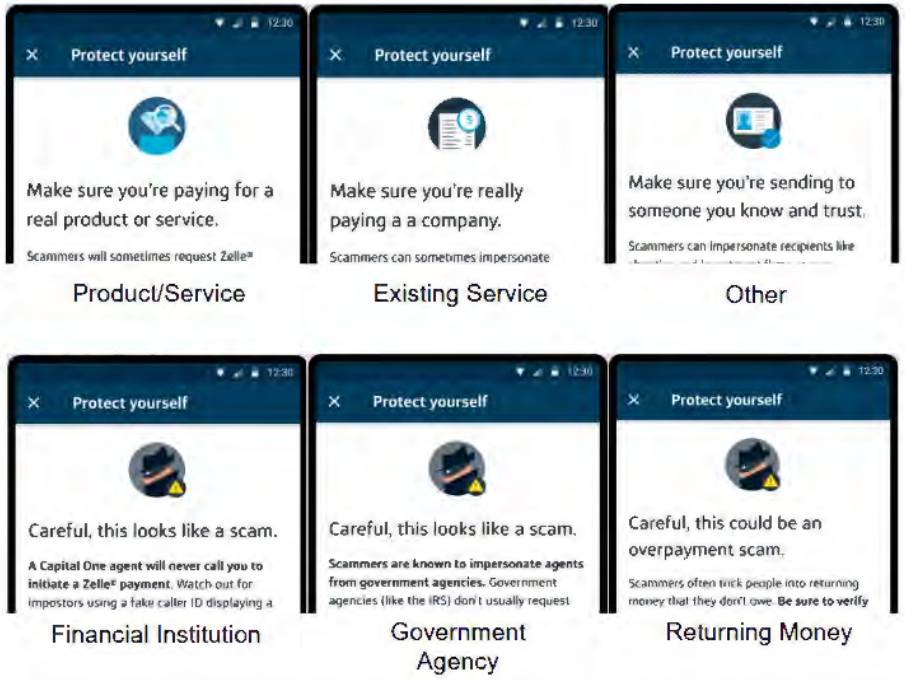
Choose a Send Reason UX

Adding a new recipient during the Zelle send flow triggers the Choose a Send Reason UX



Scenario Selection

The customer's selection drives tailored warnings, including preventing customers from proceeding in certain scenarios

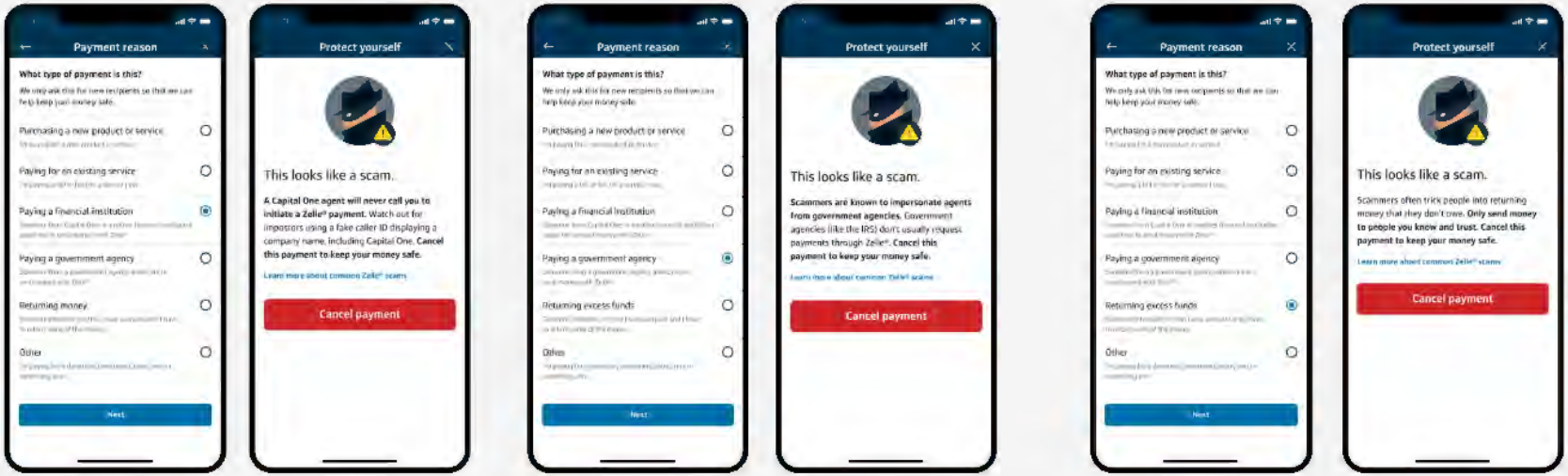


Product/Service | Existing Service | Other

Financial Institution | Government Agency | Returning Money

In the highest scam risk scenarios, customers are directed to cancel payments

Choose a Send Reason UX



Education/Prevention

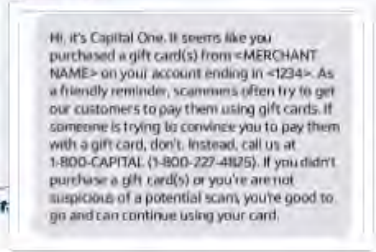
We also have three scam alerts in market that target risky behaviors

Fraud101

In Market

Gift Card Scam Alert

- 1-Way, email & text educating customer on gift card scams
- Sent to primary on gift card transactions >$400
- Averages ~7,000 alerts/month, when not in holiday season, w/ ~3% followed by a claim
- Call listening has shown both effectiveness in stopping scam, but also customers disbelieving the scam and still making the purchase


Hi, it's Capital One. It seems like you purchased a gift card(s) from <MERCHANT NAME> on your account ending in <1234>. As a friendly reminder, scammers often try to get our customers to pay them using gift cards. If someone is trying to convince you to pay them with a gift card, don't. Instead, call us at 1-800-CAPITAL (1-800-227-4825). If you didn't purchase a gift card(s) or you're are not suspicious of a potential scam, you're good to go and can continue using your card.

Risky Payment Alert

- 1-Way, email & text educating customer on payment scams
- Triggered by Risky Login report, which looks for payments made after a digital login from high risky time zones, ~40% hit rate
- Averages ~500 alerts/month
- Early reads show decreases in both returned payment amounts (24%) and DQ rates (17%)

Rip Off Reminder

- $18M of approved auths are made with scam merchants each month – only ~10% of these dollars are claimed
- This 1-Way email alert would ask customers w/ approved auths at blocked merchants if they want to submit a claim digitally
- Initial test would keep annual exposure <$50K

Industry leading authentication methods protect customers from fraud

New Authentication Methods

Government ID + Selfie / Liveness

Tap your Debit Card

Interactive One-time PIN