REPORT

THE SCAM EPIDEMIC AND THE FEDERAL CRACKDOWN TO COMBAT IT

A FOLLOW-UP TO ZELLE AND THE ART OF COMBATING DIGITAL SCAMS

UNLEASH PROSPERITY NOW

Date :

JUNE 2026

Prepared by :

UNLEASH PROSPERITY NOW
STEPHEN MOORE

The Scam Epidemic and the Federal Crackdown to Combat It

A Follow-Up to Zelle and the Art of Combating Digital Scams

Introduction

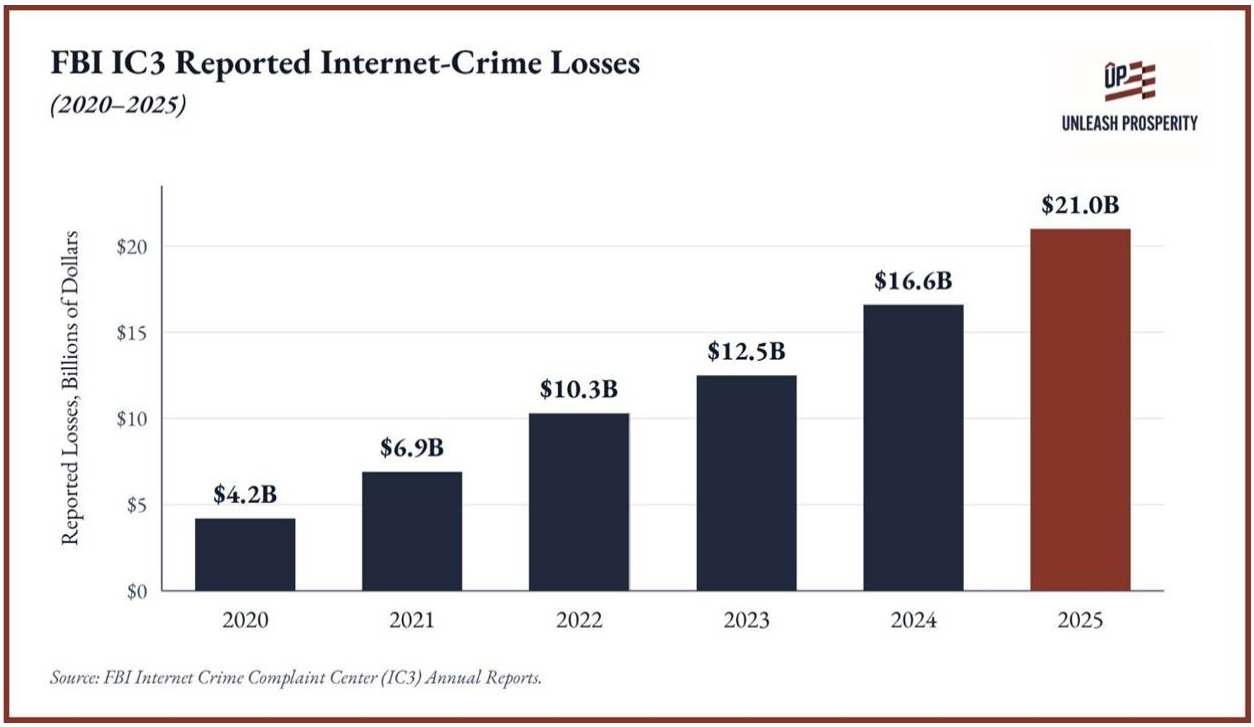
Last year, we published *Zelle and the Art of Combating Digital Scams*, highlighting the Biden administration's misguided and politically motived action in the waning days of Rohit Chopra's time at the Consumer Financial Protection Bureau. The Trump Administration has taken a more pragmatic approach to the fraud and scam problem by working to address the root cause. This is needed since, scams against Americans have only accelerated. The FBI now reports that cyber-enabled crime drained close to $21 billion from Americans in 2025, the highest figure ever recorded[1]. The Federal Trade Commission reports that losses to scams originating on social media have climbed eightfold since 2020[2]. Furthermore, a large and growing share of this theft is run out of industrial scam compounds in Southeast Asia, staffed by trafficked labor and powered increasingly by artificial intelligence.

This follow-up study turns from defense to offense. We document the scale of the threat, and we argue that the current administration has already begun doing what is needed to address it. In its first year, the Trump administration designated foreign cartels as terrorist organizations[3], sanctioned the financial backbone of the Southeast Asian scam economy[4], executed the largest forfeiture action in the history of the Justice Department[5], and formed a dedicated interagency Scam Center Strike Force[6]. These are precisely the kinds of coordinated, source-focused actions we called for last year. The task now is to sustain them, resource them, and widen their reach.

The scam problem is real and demands a response. It is not caused by companies or payment platforms like Zelle, and it will not be solved by overregulating them. The true source of the problem is sophisticated criminal enterprises operating largely beyond our borders. We can only solve this problem by going after those enterprises with the full weight of federal law enforcement.

The Scale of the Problem Has Grown

The FBI reported $16.6 billion cybercrime and online fraud losses for 2024 from schemes like romance scams and "pig butchering". That number, alarming at the time, has already been eclipsed. The FBI's 2025 Internet Crime Report, released in April 2026, found that cyber-enabled crimes defrauded Americans of nearly $21 billion[7]. The Internet Crime Complaint Center received more than one million complaints for the first time in its history, 1,008,597 in all, up from 859,532 the year before. The center now fields roughly 3,000 complaints every single day.[8]



In the span of five years, annual reported losses have multiplied roughly fivefold. And these figures likely understate reality, as victims chronically underreport fraud out of embarrassment or a belief that nothing can be done. The true national toll is higher than any single agency captures, a point the Government Accountability Office has made repeatedly in calling for a unified federal estimate that still does not exist.[9]

Of those victimized by these crimes, older Americans are hit hardest. Those over 60 years of age reported approximately $7.7 billion in losses in 2025, a 37 percent jump from the prior year[10]. These are often retirees losing savings they cannot rebuild.

Artificial Intelligence and Social Media

What separates the threat of 2026 from the threat of 2024 is not merely scale but method. Generative artificial intelligence and the reach of social media platforms have supercharged the scam economy.

Artificial Intelligence Enters the Fraud Toolkit

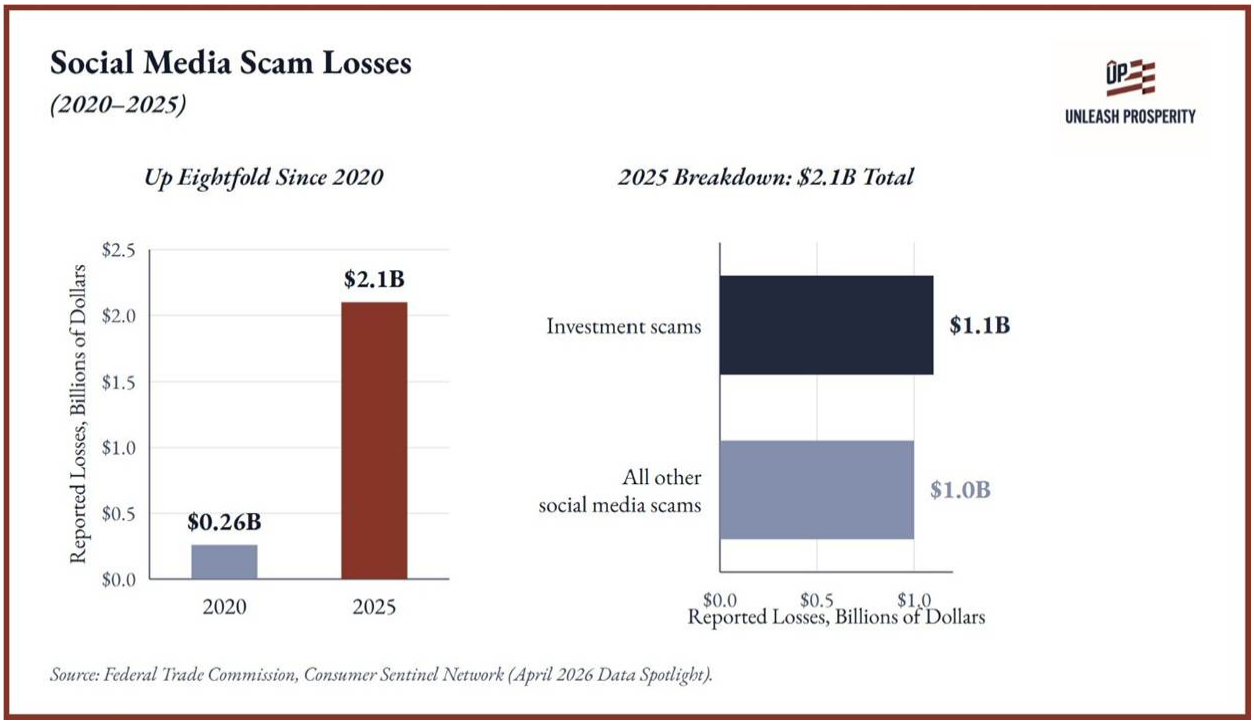
The FBI's latest annual crime report devotes a dedicated section to artificial intelligence ("AI"). AI has handed criminals a set of tools that make their schemes faster, cheaper, and far more convincing. In 2025, AI-related complaints numbered 22,364 and cost Americans nearly $893 million[11]. Scammers now deploy voice clones of family members, fabricated identification documents, fake social media profiles generated at scale, and deepfake videos depicting public figures or loved ones to manufacture trust and urgency.

A scammer no longer needs to speak fluent English, a convincing photograph, or a plausible backstory. A single operator can run hundreds of simultaneous conversations, each one personalized. The Cambodian scam

compounds described later in this study reportedly run "phone farms" with large numbers of devices using AI tools to operate fraudulent accounts at industrial scale. Much of this work is now automated, and the tools are still improving.

Social Media Has Become the Costliest Point of Contact

In 2025, nearly 30 percent of people who reported losing money to a scam said it began on social media, with reported losses reaching a staggering $2.1 billion. That represents an eightfold increase since 2020, larger than any other contact method.[12]



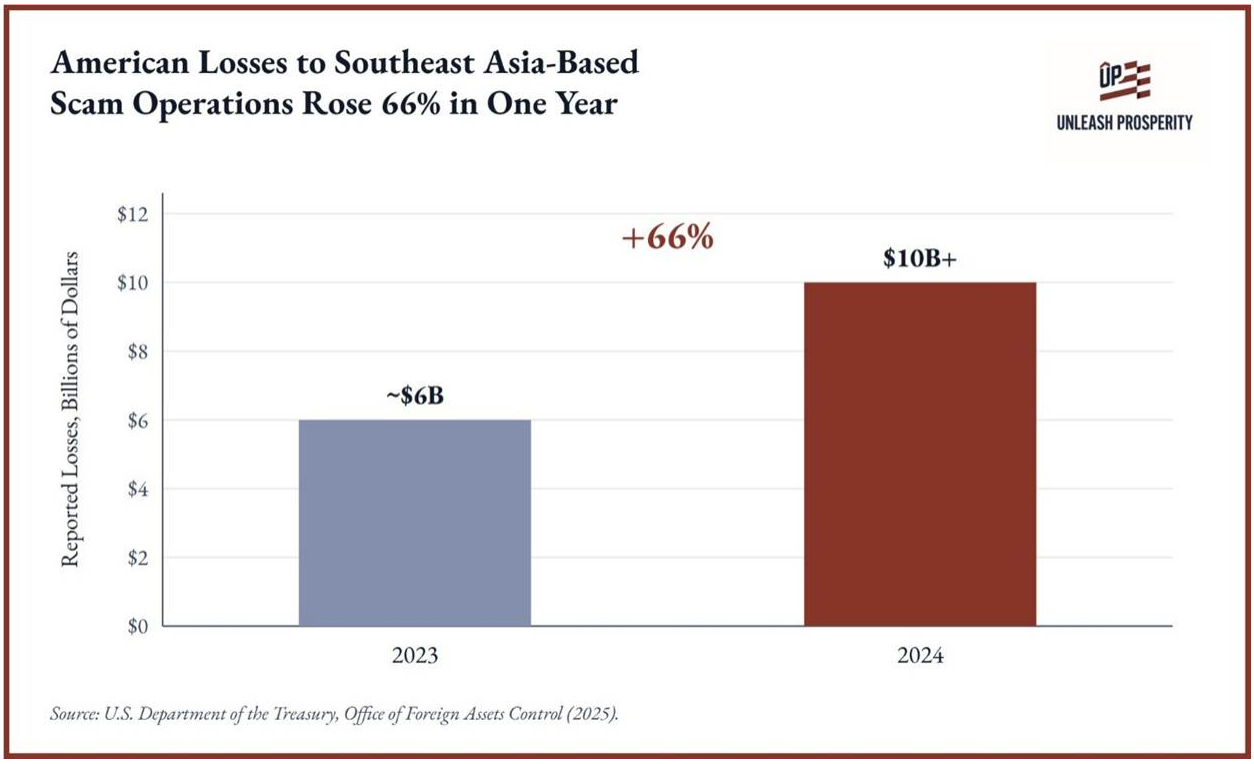
Social media offers instant, low-cost access to billions of people anywhere in the world. Scammers hack existing accounts, mine public posts to tailor their approach, or simply buy advertising and use the same audience-targeting tools legitimate businesses rely on. The FTC's data show these scams are concentrated in three categories. Investment scams led the way at $1.1 billion, more than half of all social media losses, frequently beginning with an ad or post promising to teach people how to invest. Shopping scams were the most frequently reported, with more than 40 percent of social media fraud victims saying they had ordered something advertised on a platform that never arrived or arrived as a counterfeit. And romance scams, with nearly 60 percent of people who lost money to a romance scam in 2025 saying it started on a social media platform.[13]

Notably, people reported losing more money to scams that started on Facebook alone than to text or email scams combined. Every age group except those 80 and over reported losing more to social-media-originated scams than to any other contact method.

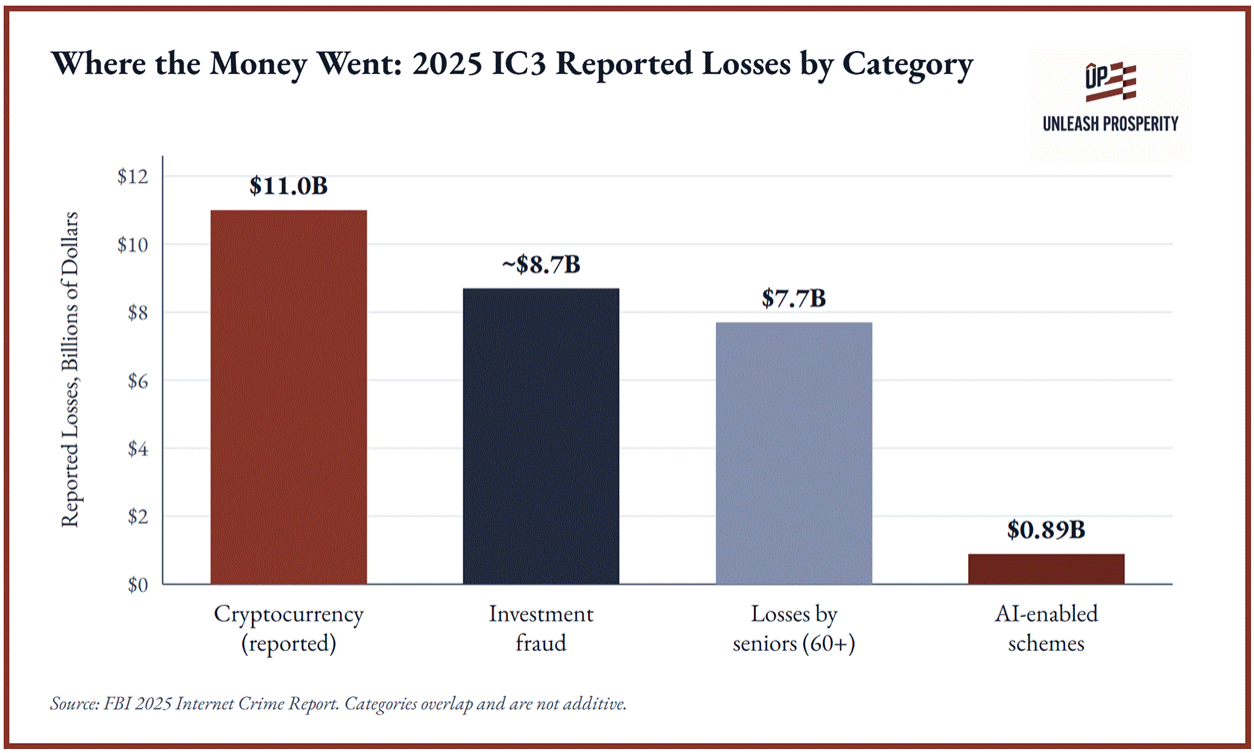
The International Engine of the Scam Economy

Our first study demonstrated that fraud on platforms like Zelle arises from "increasingly clever and sophisticated global criminal networks" rather than from any flaw in the platforms themselves. Over the past year, the federal government has put hard numbers and specific names to those criminal networks.

The Treasury Department estimates that Americans lost at least $10 billion to Southeast Asia-based scam operations in 2024, a 66 percent increase over the prior year[14]. These are not loose collections of individual fraudsters. They are organized enterprises that build and operate fortified compounds across Cambodia, Burma, and Laos, staffed in large part by workers trafficked under false pretenses and held through debt bondage, physical violence, and threats. The workers are forced to run "pig butchering" scams, in which operators "fatten" victims with attention and false affection before draining their savings through fake cryptocurrency investment platforms.



Cryptocurrency is a key component of these scam operations. Of all the loss categories the FBI tracked in 2025, complaints involving cryptocurrency were the costliest, with 181,565 complaints totaling more than $11 billion. Investment fraud, the category these pig-butchering operations fall under, accounted for nearly half of all scam-related losses.[15] Crypto's speed and international reach make it the preferred vehicle for moving stolen funds out of the United States.



There is, however, an advantage for investigators. The same blockchain technology criminals exploit also leaves a permanent, traceable record. Unlike cash, cryptocurrency transactions can be followed. That traceability is precisely what has allowed federal investigators to map these networks end to end, from the first contact with a victim through the laundering of proceeds, and to seize funds at a scale that was previously impossible.

The Federal Crackdown Is Working

The central recommendation of our first study was the creation of a coordinated, multi-sector effort that would break down the silos between banking regulators, law enforcement, telecom authorities, and private industry and go after fraud at its true source. Over the past year, the administration has adopted this strategy and put it to work. The results so far are significant.

Treating Transnational Crime as a National Security Threat

Executive Order 14157, signed January 20, 2025, created the process to designate international cartels and transnational criminal organizations as Foreign Terrorist Organizations and Specially Designated Global Terrorists[16]. On February 20, 2025, the State Department formally designated eight such organizations, including the Sinaloa Cartel, Cartel de Jalisco Nueva Generacion, Tren de Aragua, and MS-13[17]. The practical effect is that anyone who knowingly provides material support to these groups faces terrorism-related criminal exposure, and foreign financial institutions that handle their money risk secondary sanctions that can cut them off from the U.S. financial system.

This is significant for scam enforcement because it establishes both a template and a set of tools. The same instruments now being aimed at drug cartels, terrorism designations, asset forfeiture, secondary sanctions, and aggressive Treasury action, are exactly the instruments suited to dismantling transnational scam syndicates. The bold posture the administration took against South American cartels is the model worth extending to the criminal enterprises targeting Americans through their phones.

Cut Off the Money: Treasury and OFAC Actions

Treasury has moved aggressively against the financial infrastructure of the scam economy. In May 2025, the Financial Crimes Enforcement Network identified Cambodia's Huione Group as a primary money laundering concern under Section 311 of the USA PATRIOT Act. Huione had served as a critical hub for laundering proceeds from pig-butchering scams and North Korean cyber heists, with more than $4 billion in illicit funds flowing through its platforms[18]. In September 2025, the Office of Foreign Assets Control sanctioned nineteen entities and individuals across Burma and Cambodia tied to large-scale crypto investment fraud.[19] in 2024 unsuspecting Americans lost over $10 billion to Southeast Asia-based scams, leading Treasury Under Secretary John K. Hurley to state that under the current leadership Treasury would "deploy the full weight of its tools to combat organized financial crime and protect Americans."

Big Wins in Justice Department History

In October 2025, the United States and the United Kingdom imposed coordinated sanctions on 146 individuals and entities tied to the Prince Group, a transnational criminal organization that ran scam compounds across Cambodia[20]. Simultaneously, the Justice Department unsealed an indictment against Chen Zhi, the group's chairman, on charges of wire fraud and money laundering conspiracy, and filed a forfeiture action against approximately 127,271 Bitcoin, worth roughly $15 billion. This represents largest forfeiture action in the history of the Department of Justice[21]. Prosecutors described the operation as one of the largest investment fraud schemes in history, and noted that at its peak Chen allegedly bragged the scam was pulling in $30 million a day.

Rather than burdening domestic banks and payment apps with liability for crimes committed by foreigners, the government identified the criminal enterprise, followed the cryptocurrency, froze the proceeds, and charged the true perpetrators of the crime. It is the approach we advocated, executed at a scale few would have predicted was even possible a year ago.

The Task Force We Proposed in Action

In November 2025, the U.S. Attorney for the District of Columbia, together with the FBI and the Secret Service, announced the creation of a Scam Center Strike Force. This is a dedicated interagency task force to investigate, disrupt, and prosecute the most egregious Southeast Asian scam centers and their leaders. The Strike Force works alongside Treasury's OFAC, the State Department, and other agencies, combining sanctions, seizures, and criminal prosecution. It has already seized more than $401 million in cryptocurrency and is pursuing an additional $80 million in forfeiture intended for return to victims.[22]

We called for an interagency body co-chaired by law enforcement and financial regulators, drawing on the distinct authorities and data of each, focused on coordinated disruption rather than blunt regulation, and

committed to victim restitution. The Scam Center Strike Force is a substantial step in that direction. Alongside it, the FBI's Operation Level Up, launched in 2024 to proactively notify Americans actively being defrauded, has surpassed 8,000 victims notified and reduced losses by more than $500 million[23]. In 2026, the Bureau added Operation Winter SHIELD to help organizations harden their defenses.

A Source-Focused Approach Is the Solution

The prior administration's instinct was to push liability onto the domestic institutions closest to the consumer. The current approach goes after the criminals committing the fraud. This approach actually produces results.

Victims gain more from the seizure of $15 billion and the return of forfeited funds than they would from shifting blame and cost onto financial institutions or companies. Consumers are spared higher prices on the free payment tools that tens of millions of people, including low-income households, depend on. Financial technology firms are not saddled with open-ended liability for crimes committed by third parties overseas. And the approach reduces fraud more effectively, because it strikes at the enterprises generating the losses rather than at the channels through which the money happens to move.

Mandating blanket reimbursement would have created a moral hazard problem, inviting potential abuse while doing nothing to disrupt the compounds in Cambodia and Burma actually running the scams. A criminal in a Shwe Kokko compound does not care which domestic bank reimburses the victim. He cares whether his compound is sanctioned, his crypto wallet frozen, and his boss indicted.

Recommendations

The administration has the right strategy. The priority now is to institutionalize and extend it so that the gains of the past year compound rather than fade. We offer the following recommendations.

Make the Scam Center Strike Force permanent and well-resourced. Ad hoc task forces dissolve when attention shifts. The Strike Force should be given durable statutory footing, dedicated funding, and personnel detailed from Treasury, DOJ, FBI, the Secret Service, State, and FinCEN, with clear authority to coordinate across all of them. Its mandate should explicitly include returning forfeited assets to victims.

Lean further into cryptocurrency tracing. The blockchain's traceability has been a decisive law enforcement advantage. Treasury and DOJ should expand their blockchain-analytics capacity and deepen partnerships with private analytics firms, while resisting calls to drive these transactions into less traceable channels.

Engage the financial sector as a partner. Banks and payment platforms hold rich data on fraud patterns and can freeze suspicious transfers quickly when alerted. The right posture is collaboration: real-time intelligence sharing with safe harbors, faster fund-freeze protocols when law enforcement flags an account, and joint analytics. This is the public-private model that punitive regulation would have foreclosed.

Treat major scam syndicates with the same seriousness as cartels. The terrorism-designation framework applied to drug cartels offers a proven set of tools. Where transnational scam organizations meet the

criteria, the administration should not hesitate to bring the full apparatus of designation, secondary sanctions, and forfeiture to bear against them.

Confront the AI and social media threat directly. Platforms should be pressed to act faster against fraudulent advertising and impersonation accounts, and to give consumers better tools to verify who they are dealing with. A coordinated public-education campaign, leveraging both government and industry channels, should warn Americans specifically about AI voice clones, deepfakes, and investment pitches that arrive through social media feeds.

Build the unified national fraud estimate requested by GAO. The government still has no single, authoritative count of scam losses. The discrepancy between agency figures obscures the true scale and hampers resource allocation. A harmonized estimate, owned by the Strike Force or a designated lead agency, would be a significant step in the right direction.

Conclusion

Last year we argued that the government was aiming at the wrong target. The 2025 data proves we were right. The scam epidemic is real, it is growing, and it is driven by international syndicates wielding cryptocurrency, artificial intelligence, and the global reach of social media.

The encouraging news is that the federal government has, over the past year, begun to fight this fight the right way. Policy makers should now focus on the following five points.

1. The scam threat is larger than ever and still growing. Reported losses approached $21 billion in 2025, and the real figure is likely higher. This is a national problem deserving of sustained national attention.

2. The fraud originates with criminals, not with payment platforms. The case for overregulating Zelle and its peers was weak a year ago and is weaker now that the true source of the losses has been widely exposed.

3. Artificial intelligence and social media have changed the nature of the threat. Voice clones, deepfakes, and platform-targeted advertising have made scams cheaper to run and harder to detect, and the response must keep pace.

4. The administration's source-focused crackdown is working. Terrorism designations, Treasury sanctions, the largest forfeiture in DOJ history, and a dedicated Scam Center Strike Force represent exactly the coordinated, offensive strategy this problem demands.

5. The right course is to sustain and widen the offensive, not to retreat into burdensome regulation. Make the Strike Force permanent, press the cryptocurrency-tracing advantage, partner with the financial sector, and confront the AI and social media threat head on.

Protecting Americans' financial security does not require throttling the innovations that have made moving money cheap, fast, and accessible. It requires going after the people stealing the money. The current administration has shown over the past year that it knows how to do this. It should keep going.

[1]FBI National Press Office, "Cryptocurrency and AI Scams Bilk Americans of Billions," April 6, 2026. https://www.fbi.gov/news/press-releases/cryptocurrency-and-ai-scams-bilk-americans-of-billions

[2]Federal Trade Commission, "New FTC Data Show People Have Lost Billions to Social Media Scams," April 27, 2026. https://www.ftc.gov/news-events/news/press-releases/2026/04/new-ftc-data-show-people-have-lost-billions-social-media-scams

[3]U.S. Department of State / OFAC, designations of eight cartels and transnational criminal organizations as FTOs and SDGTs, effective February 20, 2025. https://www.state.gov/terrorist-designations-of-international-cartels/

[4]U.S. Department of the Treasury, Office of Foreign Assets Control, sanctions targeting Southeast Asian scam networks, September 8, 2025. https://home.treasury.gov/news/press-releases/sb0237

[5]U.S. Department of Justice, "Chairman of Prince Group Indicted for Operating Cambodian Forced-Labor Scam Compounds Engaged in Cryptocurrency Fraud Schemes," October 14, 2025. https://www.justice.gov/opa/pr/chairman-prince-group-indicted-operating-cambodian-forced-labor-scam-compounds-engaged

[6]U.S. Attorney's Office, District of Columbia, with the FBI and U.S. Secret Service, establishment of the Scam Center Strike Force, November 12, 2025. https://www.justice.gov/usao-dc/scam-center-strike-force

[7]FBI National Press Office, "Cryptocurrency and AI Scams Bilk Americans of Billions," April 6, 2026. https://www.fbi.gov/news/press-releases/cryptocurrency-and-ai-scams-bilk-americans-of-billions

[8]FBI, 2025 Internet Crime Report (IC3), released April 2026. https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf

[9]U.S. Government Accountability Office, "Fraud Risk Management: 2018-2022 Data Show Federal Government Loses an Estimated $233 Billion to $521 Billion Annually to Fraud," GAO-24-105833, April 16, 2024. https://www.gao.gov/products/gao-24-105833

[10]FBI National Press Office, "Cryptocurrency and AI Scams Bilk Americans of Billions," April 6, 2026. https://www.fbi.gov/news/press-releases/cryptocurrency-and-ai-scams-bilk-americans-of-billions

[11]FBI National Press Office, "Cryptocurrency and AI Scams Bilk Americans of Billions," April 6, 2026. https://www.fbi.gov/news/press-releases/cryptocurrency-and-ai-scams-bilk-americans-of-billions

[12]Federal Trade Commission, "New FTC Data Show People Have Lost Billions to Social Media Scams," April 27, 2026. https://www.ftc.gov/news-events/news/press-releases/2026/04/new-ftc-data-show-people-have-lost-billions-social-media-scams

[13]FTC Data Spotlight, "Reported losses to scams on social media eight times higher than in 2020," April 2026. https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2026/04/reported-losses-scams-social-media-eight-times-higher-2020

[14]U.S. Department of the Treasury, Office of Foreign Assets Control, sanctions targeting Southeast Asian scam networks, September 8, 2025. https://home.treasury.gov/news/press-releases/sb0237

[15]FBI National Press Office, "Cryptocurrency and AI Scams Bilk Americans of Billions," April 6, 2026. https://www.fbi.gov/news/press-releases/cryptocurrency-and-ai-scams-bilk-americans-of-billions

[16]The White House, Executive Order 14157, "Designating Cartels and Other Organizations as Foreign Terrorist Organizations and Specially Designated Global Terrorists," January 20, 2025. https://www.whitehouse.gov/presidential-actions/2025/01/designating-cartels-and-other-organizations-as-foreign-terrorist-organizations-and-specially-designated-global-terrorists/

[17]U.S. Department of State / OFAC, designations of eight cartels and transnational criminal organizations as FTOs and SDGTs, effective February 20, 2025. https://www.state.gov/terrorist-designations-of-international-cartels/

[18]U.S. Department of the Treasury, Financial Crimes Enforcement Network, identification of Huione Group as a financial institution of primary money laundering concern under Section 311 of the USA PATRIOT Act, May 1, 2025 (finalized October 15, 2025). https://home.treasury.gov/news/press-releases/sb0278

[19]U.S. Department of the Treasury, Office of Foreign Assets Control, sanctions targeting Southeast Asian scam networks, September 8, 2025. https://home.treasury.gov/news/press-releases/sb0237

[20]U.S. Department of the Treasury, U.S. and U.K. coordinated action targeting cybercriminal networks in Southeast Asia, October 14, 2025. https://home.treasury.gov/news/press-releases/sb0278

[21]U.S. Department of Justice, "Chairman of Prince Group Indicted for Operating Cambodian Forced-Labor Scam Compounds Engaged in Cryptocurrency Fraud Schemes," October 14, 2025. https://www.justice.gov/opa/pr/chairman-prince-group-indicted-operating-cambodian-forced-labor-scam-compounds-engaged

[22]U.S. Attorney's Office, District of Columbia, with the FBI and U.S. Secret Service, establishment of the Scam Center Strike Force, November 12, 2025. https://www.justice.gov/usao-dc/scam-center-strike-force

[23]FBI, Operation Level Up victim-services initiative. https://www.fbi.gov/how-we-can-help-you/victim-services/national-crimes-and-victim-resources/operation-level-up