UNLEASH PROSPERITY

May 2025

Zelle and the Art of Combating Digital Scams

Stephen Moore and the staff of Unleash Prosperity

Stephen Moore

Chairman and Co-Founder of Unleash Prosperity

Introduction

The Zelle platform for consumer financial transactions has been a spectacular success with American consumers since it emerged on the scene in 2016. Its cost to consumers is close to zero and the number and value of Zelle money transfers has increased more than 10-fold. The market has spoken loud and clear: Americans like using Zelle. If ever there were a new product that has benefited American consumers, it is this one.

So there is rich irony that last December the federal agency called the Consumer Financial Protection Bureau (CFPB) filed a lawsuit against Early Warning Services (EWS)—the operator of Zelle—and three major banks: Bank of America, JPMorgan Chase, and Wells Fargo. Talk about no good deed going unpunished. The lawsuit alleged that these institutions failed to implement adequate safeguards against fraud on the Zelle platform. The CFPB accused the banks of neglecting to properly investigate fraud complaints and of violating the Electronic Fund Transfer Act by not reimbursing victims of unauthorized transactions.

Those charges were dropped on March 4, 2025, under the direction of Acting Director Russell Vought. The CFPB dismissed the lawsuit with prejudice, barring a refiling of the suit, and averted a potentially disastrous regulatory misstep.

The worry is that by placing Zelle in its regulatory crosshairs the CFPB has creaked open the door to further regulatory interventions by the more than five regulatory agencies that have oversight of financial and banking institutions. This will become a bigger risk as Zelle grows in influence in the money transfer market.

The regulations that are contemplated could wind up disrupting the availability of this new and popular product while raising costs for consumers.

What Is the Case Against Zelle?

As a peer-to-peer payment platform, Zelle operates as an intermediary, facilitating secure and rapid financial transactions for American consumers and businesses. It also has an admirable record of preventing fraud. Yet, it found itself at the center of an inquiry into fraud reimbursement practices, despite abundant evidence that fraudulent activity arises from external bad actors, not from any inherent flaws in Zelle's system or business practices.

Fraud occurs in this market as increasingly clever and sophisticated global criminal networks exploit vulnerable consumers, and yet the CFPB risked punishing Zelle for circumstances beyond its control. This approach would have crippled innovation, increased costs for consumers, and undermined accessibility to financial payment systems - particularly for low-income users who depend on Zelle's free financial services.

Although the CFPB stood down, the question of how to address the systemic issue of financial fraud still lingers. What is needed is customer protections that don't threaten to grind these financial platforms to a halt due to costly and ineffective regulation.

In this study, we chart a path to answering this question by first providing a post-mortem analysis on what the economic and legal consequences might have been had the CFPB's lawsuit been pursued further. We then document the scope of fraud in the market (with relevant data from the FBI, FTC, GAO, etc.), highlighting gaps and challenges in the current fragmented approach to combating financial fraud.

One potential solution is a public–private task force or advisory commission to address the problem at its true source. The proposed task force would unify data, align enforcement, and promote consumer-centered education without punishing financial platform intermediaries. The end goal is a national strategy that leverages law enforcement, industry, and consumer groups to coordinate their efforts to reduce scams and protect Americans' financial security.

Legal Overreach and Abuse of Power

Although it is no longer an immediate threat, the Consumer Financial Protection Bureau's investigation into Zelle raises significant concerns about regulatory overreach.

Zelle's structure and operations, which facilitate direct bank-to-bank transfers, are in clear compliance with UDAAP principles. Fraudulent activities on the platform typically arise from user error or manipulation by external bad actors rather than deficiencies in Zelle's system. By investigating Zelle under UDAAP provisions, the CFPB risked conflating third-party criminal behavior with corporate misconduct, dangerously stretching the boundaries of its regulatory authority.

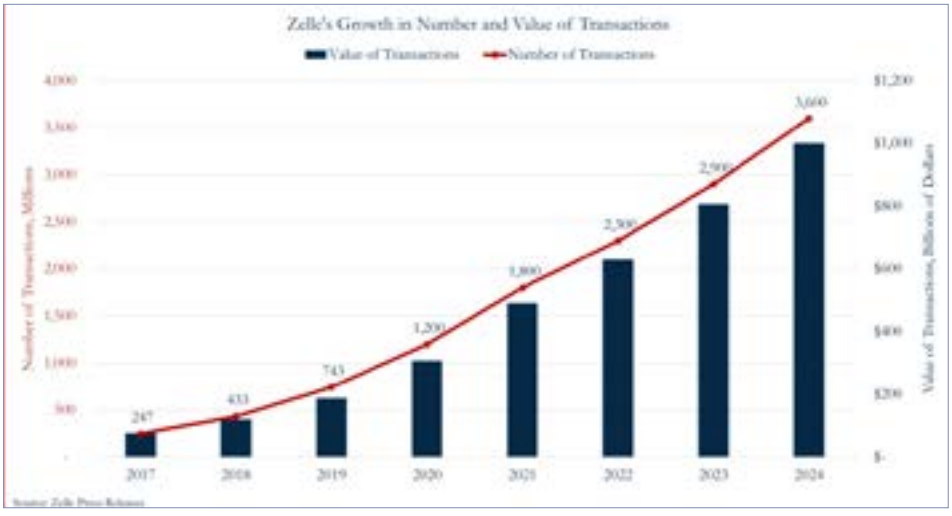
The agency's push to hold Zelle and its participating banks accountable for all fraud losses undermines the platform's fundamental design and consumer agreements. Ironically, a pro-consumer regulatory intervention in this case will only raise prices and on or deny service access to the very consumers that are supposed to be helped

The initial impulse by regulators to impose blanket liability for fraud would also have been a departure from established norms governing consumer responsibility in electronic payment systems, such as those codified under the Electronic Fund Transfer Act (EFTA).

Regulatory Overreach and Market Implications

It is vital to point out that even with the small risk of fraudulent transfers, the popularity of Zelle has exploded in the last decade with volume up an order of magnitude and growing every year. Excessive regulation threatens to erase billions of dollars of consumer value from these services.

From 2017 to 2024, the number of transactions on Zelle vaulted from under 250 million to 3.6 billion. During that period, the value of transactions on Zelle increased at an average annual rate of over 31%. Zelle is also integrated with over 2,000 financial institutions, highlighting its importance as a tool for seamless financial inclusion. The immense value that Zelle provides for consumers and financial institutions is unmistakable and any regulatory interventions that unfairly increase operational costs could deter investment in similar technologies, stifling competition and limiting consumer choice.



Economic Incentives and Fraud Risk

Encouraging Fraud Through Coerced Reimbursement Policies

Regulators have also missed the point that enforcing mandatory fraud reimbursement policies would inadvertently encourage fraudulent activities. In economic theory, creating systems with guaranteed reimbursements diminishes personal accountability, increasing the likelihood of abuse. Customers will be less attentive to risks of fraud if the risks are entirely borne by the banks. Fraudsters may exploit lenient refund policies by using stolen credentials for unauthorized transfers, banking on the fact that victims will be promptly reimbursed. This phenomenon, also known as the Peltzman effect, creates a moral hazard problem, where insulating individuals from risk, leads to increased unwanted behaviors.

Data from similar payment systems illustrates this risk. Venmo and Cash App, which face fewer fraud-related reimbursement constraints, experience fraud rates comparable to or exceeding Zelle's.[1] By contrast, Zelle has maintained robust fraud prevention measures, emphasizing education and technological safeguards rather than blanket refund guarantees. Expanding mandatory reimbursements could undermine these efforts, burdening participating banks with increased fraud-related costs and deterring their future investments in anti-fraud technologies.

Zelle's Fraud Risks Compared to Industry Norms

What is amazing about this whole debate about the need for regulatory intervention is that Zelle reports that 99.95% of its transactions occur WITHOUT fraud or scams, a statistic that aligns with or surpasses the security performance of other peer-to-peer platforms. The platform's fraud risks are inherently mitigated by its direct integration with banking institutions, which employ sophisticated authentication protocols and account monitoring systems. Unlike competitors that rely on intermediary wallets, Zelle's design limits exposure to fraudulent schemes by eliminating redundant steps where bad actors might prey on unsuspecting consumers.

Furthermore, evidence suggests that fraud rates in the banking sector, including online and card payment fraud, are not disproportionately lower than those associated with P2P systems like Zelle. This underscores that fraud is a pervasive problem and in no way exclusive to P2P systems.

It is also worth mentioning that the federal government made $236 billion worth of "improper payments" or arguably fraudulent payments in FY2023, accounting for 3.58% of all federal payments for the year.[2] Its rate of fraud is multiple times higher than that of Zelle. In fact the government might be well-served to prevent taxpayer fraud by contracting with peer-to-peer services like Zelle that are much better at screening out criminal behavior or other forms of theft.

---

1 https://www.americanbanker.com/news/comparing-fraud-zelle-vs-venmo-vs-paypal-vs-cash-app-vs-apple?utm_source=chatgpt.com

2 https://www.gao.gov/blog/federal-government-made-236-billion-improper-payments-last-fiscal-year

Consumer Cost Implications

The Economic Value of Free Services for Low-Income Users

Zelle's cost-free service model is a critical financial tool for millions of Americans, especially low-income individuals who depend on affordable payment solutions. Unlike traditional wire transfers or checks, which incur fees and delays, Zelle enables instantaneous, fee-free transfers directly between bank accounts. This functionality reduces financial barriers, making it easier for users to manage expenses, split bills, or remit funds to family members without incurring additional costs.

Regulatory pressure to enforce liability for fraud would undermine this model by increasing operational costs for banks. To offset these expenses, banks would be forced to introduce service fees or restrict access to Zelle, disproportionately affecting low-income users. The loss of a free payment option would force many to revert to high-cost alternatives such as money orders or payday loans, exacerbating existing financial inequities.

Cost Comparisons Across Payment Ecosystems

Zelle's ability to operate without user fees is particularly significant in an ecosystem where most P2P payment platforms monetize their services. Venmo and Cash App, the other two major platforms in the P2P space, charge fees for instant transfers or premium features, which can add up over time for frequent users. By contrast, Zelle's integration into existing bank infrastructures allows it to offer services without imposing such charges on its users. This unique model benefits a wide demographic, from small business owners who rely on seamless payments to low income populations seeking low-cost financial tools.

If fraud-related liabilities force Zelle to implement fees or scale back operations, the resulting economic harm would ripple across these user groups. Users who are priced out of the platform would face limited financial options, widening the digital divide and unnecessarily excluding marginalized consumers.

The Growing Scam Threat

Although the CFPB's actions were misguided, the underlying problem of financial fraud and consumer scams remains a legitimate and pervasive problem. Multiple official sources confirm the crisis. The FBI's Internet Crime Complaint Center (IC3) received 880,418 complaints in 2023 and 893,000 in 2024.[3] About 256,256 complaints involved actual monetary loss, with an average loss of $19,372. Reported losses continue to climb as well. In 2024 internet-crime losses reached $16.6 billion, a 33% jump from 2023.[4] And it is important to keep in mind that these figures likely understate the true extent of losses to fraud as victims generally under report fraud, in part due to embarrassment or thinking nothing can be done.

Scammers now operate across multiple channels using a wide array of strategies.

Peer-to-Peer (P2P) Payment Scams: Fraudsters exploit consumers using instant payment apps (Zelle, Venmo, Cash App, etc.). Victims often lose money via authorized transfers induced by imposters using "friend in need" or fake buyer schemes to induce victims to authorize financial transactions. Zelle and other P2P platforms post numerous consumer warnings and payment holds to slow down scams but they persist nonetheless.[5] FTC data show scams involving P2P transactions led to $1.8 billion in reported losses in 2023,[6] and in 2024 consumers lost more to scams paid via bank transfers or crypto than all other methods combined.[7]

Telecom (Robocall/Text) Scams: Robocalls and text scams remain a pervasive channel for financial fraud. The FTC reports U.S. consumers are bombarded by millions of illegal calls each month with most originating overseas and funneled through voice over internet protocol (VoIP) gateway providers.[8] Common tactics through this channel include IRS impersonation, tech support cons, and "free prize" leads that trick unsuspecting victims into giving consent to call. Enforcement groups are ratcheting up their efforts against these scams. The FTC's Operation Stop Scam Calls involved 180+ actions by

---

3 https://www.ic3.gov/AnnualReport/Reports/2023_IC3Report.pdf#:~:text=received%20a%20record%20number%20of,figures%20appear%2C%20we%20know%20they, https://www.fbi.gov/news/press-releases/fbi-releases-annual-internet-crime-report#:~:text=released%20its%20latest%20annual%20report,increase%20in%20losses%20from%202023

4 https://www.fbi.gov/news/press-releases/fbi-releases-annual-internet-crime-report#:~:text=released%20its%20latest%20annual%20report,increase%20in%20losses%20from%202023

5 https://www.gao.gov/assets/gao-24-107107.pdf#:~:text=%E2%80%A2%20Financial%20institutions%20and%20P2P,the%20legitimacy%20of%20the%20payment

6 https://www.ftc.gov/news-events/news/press-releases/2024/02/nationwide-fraud-losses-top-10-billion-2023-ftc-steps-efforts-protect-public

7 https://www.ftc.gov/news-events/news/press-releases/2025/03/new-ftc-data-show-big-jump-reported-losses-fraud-125-billion-2024#:~:text=Consumers%20reported%20losing%20more%20money,all%20other%20payment%20methods%20combined

8 https://www.ftc.gov/news-events/news/press-releases/2023/04/ftc-ramps-fight-close-door-illegal-robocalls-originating-overseas-scammers-imposters#:~:text=As%20the%20menace%20of%20unwanted,illegal%20robocalls%20originate%20from%20overseas

102 federal/state partners to target and prosecute illegal call generators and lead sellers.[9] Another FTC initiative, Project "Point of No Entry," pressures voice carriers to block illegal traffic. Despite these efforts illegal calls persist, exploiting gaps in phone networks and consent agreements.

Social Marketplaces and Online Scams: Fraud on Craigslist, Facebook Marketplace, Instagram, dating apps, and other online platforms has exploded in recent years. Scammers lure buyers with fake listings, ask sellers to pay "guarantee" fees, or cultivate romance/business relationships to extract money. FTC data shows that this channel was the launch point for the largest scam losses in 2023 – about $1.4 billion – surpassing losses from phone calls or email.[10] Because these platforms enable anonymity and rapid reach, scams can scale globally, and victims rarely recover losses. It is also worth noting that victims of these scams often hesitate to report them to law enforcement due to feelings of shame or fear of blame.

Efforts to Reduce Fraud

Multi-agencies of the government combined with private sector industry enforcement measures help reduce fraud in electronic transfers of cash:

FTC and Law Enforcement: The FTC leads consumer fraud enforcement, including telemarketing and internet scams. Recent FTC actions include Operation Stop Scam Calls with 180+ legal actions targeting call centers, "lead generators," and VoIP facilitators.[11] Additionally, project Point of No Entry targets gateways that admit overseas robocalls. The FTC also disrupts imposter websites and phishing operations. It also works to educate the public and publish scam warnings on prevalent scammer strategies.

FBI/IC3: The FBI's Internet Crime Complaint Center (IC3) aggregates internet fraud complaints. It publishes annual reports and operates a Recovery Asset Team (RAT) that partners with banks to freeze fraudulent transfers. In 2023 the RAT triggered Financial Fraud Kill Chain protocols on 3,008 incidents (preventing potential losses of $758 million) and successfully freezing $538 million for victims (71% of cases).The FBI also leads cyber investigations and international takedowns, though it notes it can only designate limited resources to addressing global fraud rings.[12]

---

9 https://www.ftc.gov/news-events/news/press-releases/2023/07/ftc-law-enforcers-nationwide-announce-enforcement-sweep-stem-tide-illegal-telemarketing-calls-us#:~:text=The%20Federal%20Trade%20Commission%20and,consumers https://www.reuters.com/business/ftc-us-regulators-crack-down-illegal-robocalls-telemarketing-2023-07-18/#:~:text=The%20crackdown%2C%20known%20as%20Operation,C

10 https://consumer.ftc.gov/consumer-alerts/2024/02/think-you-know-what-top-scam-2023-was-take-guess#:~:text=losses%20of%20%247,person%20loss%20%28%241%2C480%20average%20loss

11 https://www.ftc.gov/news-events/news/press-releases/2023/07/ftc-law-enforcers-nationwide-announce-enforcement-sweep-stem-tide-illegal-telemarketing-calls-us#:~:text=The%20Federal%20Trade%20Commission%20and,consumers, https://www.reuters.com/business/ftc-us-regulators-crack-down-illegal-robocalls-telemarketing-2023-07-18/#:~:text=The%20crackdown%2C%20known%20as%20Operation,C

12 https://www.ic3.gov/AnnualReport/Reports/2023_IC3Report.pdf#:~:text=commitment%20to%20assisting%20cyber%20victims,FBI%20remains%20appreciative%20of%20those

Financial Institutions and Payment Networks: Banks, credit unions, and P2P platforms effectively provide consumer education and warnings on scams.They have also implemented additional controls: speed bumps, transaction delays or "holds," and warning messages for large transfers. Financial Institutions and payment networks also keep careful record and detailed data on cases of reported fraud giving them useful insight on common risk factors and common vulnerabilities.

Telecommunications Industry: Carriers and telecom providers deploy call-blocking services and implement caller-ID authentication (an FCC mandate) to deter spoofing. They participate in tracebacks (Industry Traceback Group) to help identify scam call origins. Yet perfect filtering remains unattainable with new scam campaigns constantly emerging, and many carriers reporting billions of call-blocking efforts with limited visibility of success rates.[13]

Technology and Marketplace Platforms: Online marketplaces and social networks ban fraudulent accounts/listings and partner with law enforcement on major scams. However, enforcement is largely reactive (removing reported fraud ads) and varies by company. There currently is no centralized way to track marketplace scams across platforms.

Simply stated, no single federal strategy or task force coordinates all these efforts. Agencies operate under their own mandates without a unified anti-scam mission. In fact, GAO found that there is no government-wide definition of "scam" or count of national losses, and that each agency (FTC, FBI, CFPB, etc.) collects complaints independently.[14] Even data-sharing between agencies is informal. For example, the FBI noted it has "no formalized mechanism to deconflict…coordinate…share resources" among agencies on fraud investigations.[15]

Recent counter-fraud actions suggest growing coordination but only on a sporadic basis. In 2023, federal and state partners executed unprecedented joint crackdowns on telemarketing fraud. Similarly, cross-border cybercrime units have targeted investment scam rings. Still, these remain on a case by case basis.

---

13 https://www.ftc.gov/news-events/news/press-releases/2023/04/ftc-ramps-fight-close-door-illegal-robocalls-originating-overseas-scammers-imposters#:~:text=Through%20Project%20PoNE%2C%20the%20FTC,and%20filing%20lawsuits%20when%20appropriate

14 https://www.ftc.gov/news-events/news/press-releases/2023/04/ftc-ramps-fight-close-door-illegal-robocalls-originating-overseas-scammers-imposters#:~:text=Through%20Project%20PoNE%2C%20the%20FTC,and%20filing%20lawsuits%20when%20appropriate, https://fedscoop.com/government-consumer-scams-strategy-gao-report/#:~:text=The%20federal%20government%20has%20no,have%20surged%20in%20recent%20years

15 https://fedscoop.com/government-consumer-scams-strategy-gao-report/#:~:text=%E2%80%9CIn%20this

Key Agencies and Their Roles in Anti-Scam Efforts

Agency/Entity	Role in Anti-Scam Efforts
FTC (Federal Trade Commission)	Enforces consumer protection laws against fraud (imposters, telemarketing); leads nationwide actions like Operation Stop Scam Calls; coordinates "gateway" call crackdowns; publishes scam trends and education materials.
FBI/IC3	Collects internet fraud complaints; publishes annual crime reports; runs the Recovery Asset Team to freeze scam proceeds; coordinates with international law enforcement on cyber fraud.
FCC (Federal Communications Commission)	Regulates telecom providers; mandates caller ID authentication; oversees National Do-Not-Call Registry; can levy fines on abusive carriers. Coordinates with FTC on robocall traceback efforts
CFPB (Consumer Financial Protection Bureau)	Aggregates financial consumer complaints (including some fraud reports); studies fraud trends in payments; can propose consumer-protection rules for payment systems.
Financial Institutions & P2P Apps	Issue fraud alerts and consumer warnings; implement "speed bumps" or holds on suspicious transfers; work with law enforcement to trace funds (via RAT/FFKC).
Telecommunications Providers	Deploy call- and text-blocking tools; participate in trace-back of scam calls (Industry Traceback Group); develop new detection (AI spam filtering).
Online Platforms & Marketplaces	Police and remove fraudulent listings/accounts; cooperate with enforcement on fraud rings; educate users on safe trading practices.

Each of these stakeholders has unique data and authority. A formal task force would ensure these pieces fit together into an effective, and agile defense against the rapidly evolving scam threat.

Gaps, Challenges, and the Case for a Task Force

The scope and rapidly evolving nature of modern scams far outpace the current uncoordinated patchwork approach. Without a coordinated strategy, consumers remain vulnerable to the growing scam threat. Key gaps and challenges in the current approach include:

Fragmented Data and Definitions: The FTC leads consumer fraud enforcement, including telemarketing and Fragmented Data and Definitions: Each agency tracks a subset of complaints. GAO reports no common scam definition or unified data system exists, so "agencies aren't able to put an exact number on scam complaints".[16] In fact, even FBI and FTC reports on total losses differ substantially ($16.6B vs. $12.5B for 2024) because of differing categories and definitions. Without combined and harmonized data on losses to scams, policymakers cannot target resources effectively.

Jurisdictional Silos: For example, many scams span financial regulation (CFPB/FTC), law enforcement (FBI/DOJ), and state banking laws – but no single body has lead authority. Telemarketers exploit the fact that telecom and consumer laws sit in different agencies. GAO notes that although some agencies coordinate "informally," there is no "formal, government-wide basis" for collaboration on scams.[17]

Underreporting and Victim Reluctance: Many victims do not report scams due to embarrassment or misinformation. An AARP survey found victims "feel ashamed" to admit being defrauded, especially on social media or dating sites.[18] This chronic underreporting means law enforcement and regulators lack accurate visibility. In some cases victims even fear legal consequences, underscoring the need for non-punitive policies and consumer education that encourages reporting.

Rapid Technological Change: New tools (AI, encrypted messaging, and decentralized crypto) let scammers innovate faster than agencies can adapt. Both GAO and FTC have highlighted AI's role in evolving scam tactics.[19] An agile, multi-stakeholder task force with direct input from industry leaders could more quickly update guidelines and defenses against these evolving threats.

---

16 https://www.gao.gov/products/gao-25-107088#:~:text=For%20example%2C%20the%20FBI%20estimated,develop%20ways%20to%20counter%20it

17 https://fedscoop.com/government-consumer-scams-strategy-gao-report/#:~:text=%E2%80%9CIn%20this%20regard%2C%20each%20agency,wide%20basis.%E2%80%9D , https://www.gao.gov/products/gao-25-107088#:~:text=The%2013%20federal%20agencies%20GAO,their%20efforts%20to%20counter%20scams

18 https://states.aarp.org/tennessee/scammers-target-victims-on-social-media-in-tennessee#:~:text=In%202022%2C%20the%20Volunteer%20State,McNeil%2C%20AARP%20Tennessee%20state%20director

19 https://www.gao.gov/assets/gao-24-107107.pdf#:~:text=into%20sending%20money,by%20a%20person%20with%20payment, https://fedscoop.com/government-consumer-scams-strategy-gao-report/#:~:text=The%20federal%20government%20has%20no,have%20surged%20in%20recent%20years

These challenges clearly warrant a dedicated, interagency public–private task force. The proposed task force would bring together federal regulators (FTC, CFPB, FCC, FTC, DOJ, FBI), state attorneys general, financial institutions, payment networks, telecom carriers, and tech platform representatives. Its mission would be to:

Develop a Unified Strategy: Craft a government-wide anti-scam strategy and common definitions. This includes setting national targets and coordinating action plans across agencies. This would specifically broaden the FBI-led cyber fraud strategy to include telemarketing and marketplace fraud, leveraging input from industry stakeholders.

Coordinated Data Sharing and Reporting: Create an interagency framework for sharing complaints and intelligence. This could involve a central "fusion" database for scam reports (building on IC3's current model). Consistent tracking of P2P app fraud, robocalls, and marketplace scams would enable trend analysis and a quicker response to emerging scam threats.

Coordinate Enforcement and Disruption: Regular joint operations (like the FCC collaborative project" Stop Scam Calls") should be institutionalized under the task force. Some possible starting points might be synchronizing FTC, DOJ, and FCC actions against telecom scammers, or uniting state and federal efforts against bot networks. Such efforts would allow financial institutions and payment apps to commit to faster fund freezes when alerted by law enforcement, and more streamlined reimbursement protocols where feasible.

Promote Public-Private Collaboration: Encourage banks and tech platforms to share threat data with government and with each other. Establish an industry "threat council" within the task force to coordinate new security features (e.g. P2P transaction flags) and user alerts. Similarly, telecom carriers and internet companies (social media, marketplaces) would agree to protocols for removing fraudulent content and more robust tracing of scammers' communications.

Focus on Victim Support and Education: The task force would focus on implementing victim-centered policies and education efforts. This means assuring victims that they do not face an legal repercussions for reporting. For example, regulators could issue guidance that victims who cooperatively report scams won't be prosecuted (or any unwitting legal violations. The task force would oversee a unified public education campaign on scam awareness and reporting (leveraging both FTC and industry channels) and measure its impact on consumer behavior. It would also coordinate resources for victim relief funds or reimbursement programs. The goal would be to have a balanced and targeted approach, not blanket punishments that might deter reporting.

Ensure Balanced Enforcement: While dismantling criminal networks is essential, the task force should emphasize prevention and adaptability. Civil enforcement (fines, injunctions) should be applied to perpetrators and enablers (e.g. illegal robocall carriers, fraudulent app operators) without using heavy handed regulation on technology providers, of financial platforms. Agencies should also resist pressuring victims to close investigations. Instead, building trust with victims through assistance (e.g. expediting fraud claims processes) leading to more and higher quality information for law enforcement.

Recommendations

For Policymakers: Establish an Interagency Scam Prevention Task Force co-chaired by senior DOJ/FBI officials and senior financial regulators (e.g. FTC). Direct participating agencies (FTC, FCC, DOJ, FBI, CFPB, Treasury/FinCEN, etc.) to assign personnel specifically including representatives from relevant industry leaders. The task force should also provide resources for joint technology development (fraud analytics) and for victim assistance programs. Require periodic public reports on scam trends and task force outcomes.

For Industry: Financial institutions and P2P platforms should commit to active participation on the task force, sharing real-time fraud data and ensure that customers who report scams are quickly assisted. Telecom and technology companies should implement agreed-upon anti-abuse measures (e.g. SHAKEN/STIR, marketplace trust signals) and continuously update them in consultation with regulators.

For All Stakeholders: Maintain transparency and stakeholder input. Victim advocacy groups should have seats at the table. The task force's strategy should be data-driven (using complaints to guide policy) and adaptive (periodically reviewing new scam types). Above all, ensuring a consumer-centered approach through proactive education and scam prevention.

Conclusion

The CFPB's investigation into Zelle highlighted the complexities of balancing consumer protection with the need to foster innovation and accessibility in financial services. However, the agency's approach risked overstepping legal boundaries, creating economic inefficiencies, and undermining the broader goals of financial security and consumer welfare.

We believe there are five factors to be considered in terms of regulation of this industry:

1. ***Products like Zelle are Popular with Consumers Despite Fraud Risks.***

   This market will continue to grow and even come to dominate the way we transfer money. Government regulation must not throw the baby out with the regulatory bath water.

2. ***Regulatory Overreach Can Harms Consumers and Raise Prices.***

   By attempting to impose liability standards that contradict existing consumer agreements and statutory frameworks, the CFPB risked exceeding its authority and disrupting market dynamics. Zelle operates within a well-defined legal framework, and this latest attempt to redefine its responsibilities could have created detrimental legal uncertainty, discouraging further innovation in the financial technology sector.

   Moreover, mandating universal fraud reimbursements would have only further incentivized fraudulent behavior and increased operating costs for banks, which would be passed on to consumers in the form of fees or restricted services. These outcomes disproportionately harm low-income individuals who rely on free and accessible payment platforms to manage their financial lives.

3. ***The "Cost-Free" Model that Zelle Uses Will Be at Risk.***

   Zelle's cost-free model is critical to maintaining access to valuable financial tools. Regulatory interventions that increase costs would force many users into high-fee alternatives, exacerbating financial disparities. Protecting platforms like Zelle from burdensome regulations ensures continued access to affordable payment solutions while preserving competition in the digital payments market.

4. ***Placing the Risk of Fraud on the Producers Could Increase Fraud by Insulating Consumers from the Risk and Financial Burden.***

   Holding producers responsible for fraudulent activity out of their control can only encourage further fraud by making consumers more risk tolerant. Why would consumers take measures to protect themselves from fraud if they know that payment platforms will be forced to foot the bill of their risky behaviour?

5. ***Establishing an Advisory Scam Prevention Task Force Could Reduce Crime.***

   The issue of how to prevent fraud and scams without major disruption to the market can be developed by a coordinated, multi-sector task force, that can break down the silos between banking regulators, law enforcement, telecom authorities, and private industry. By aligning goals and sharing intelligence, the task force would greatly strengthen our national resilience against fraud. It is not through ineffective regulation but through unified and well-resourced coordination of law enforcement that policymakers can protect consumers and preserve confidence in digital commerce.


Chase
Zelle