September 18, 2025

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 (Docket ID OCC-2025-0009)

To Whom It May Concern:

Early Warning Services (EWS) appreciates the opportunity to respond to this Request for Information (RFI) on payments fraud mitigation strategies. As the operator of the Zelle® network and provider of fraud prevention solutions serving over 2,300 financial institutions, EWS offers unique insights into the challenges and opportunities in combating payments fraud across the U.S. financial system.

EWS was founded 35 years ago to protect the financial system and the consumers who rely upon it from fraud and risk. In 2024 alone, EWS screened $11 trillion in payments volume and prevented over $3 billion in fraudulent transactions. EWS's risk management and intelligence product solutions enable the safe opening of bank accounts and making and receiving payments for tens of millions of consumers. EWS has been so successful at deterring fraud that, across multiple administrations, the U.S. Department of Treasury and Federal Reserve have sought help from EWS to enhance the U.S. government's money transfer methods, including in relation to the FedNow payment system, Economic Impact Payments and Advance Child Tax Credits.

Zelle is a peer-to-peer (P2P) payments solution between regulated financial institutions. Since its inception in 2017, Zelle has provided consumers with greater access to, and utility for, their bank deposit accounts by providing an innovative digital means of sending and receiving money as an alternative to checks and cash. Unlike other P2P options, money sent via Zelle transfers directly from one U.S.-based insured deposit account to another using the recipient's

U.S. mobile phone number or email address without having to share sensitive financial information, such as bank account or routing numbers, and funds are not held or transferred by EWS or any other entity that is not an insured financial institution.

Zelle and the participating institutions are subject to layers of regulation and utilize extensive and advanced security measures—including continuous fraud monitoring, data encryption, and secure technologies such as biometric authentication—to protect customers' funds and maintain the privacy of account access to help users avoid fraud or scams. **Today *over 99.98%* of Zelle transactions are completed without a report of fraud or scam.** Financial institutions generally provide Zelle free to consumers. Millions of consumers and small businesses—Zelle has over 150 million enrolled users—rely on Zelle to make essential everyday payments.

Given EWS's experience and expertise in payments and with addressing fraud and scams, our response emphasizes the critical importance of real-time collaboration, standardized data sharing, and comprehensive industry and government-wide approaches to fraud prevention that balance consumer protection with innovation in digital payments. EWS looks forward to working together with the OCC, Federal Reserve, the FDIC, and other authorities to combat payments fraud and scams. Here are the most valuable considerations for accomplishing that goal:

1. Develop a national task force to coordinate fraud detection, prevention and mitigation efforts across the ecosystem;
2. Standardize information sharing among stakeholders with an emphasis on information that can prevent losses;
3. Enhance the engagement and prevention practices of telecommunication, AI (artificial intelligence), social media, and online marketplaces to include scam origination through phone, email, text, social media, and online marketplaces, each of which is growing increasingly sophisticated with the use of advanced AI tools by criminals;
4. Increase law enforcement coordination and engagement, including by increasing funding and resources for law enforcement, expanding global enforcement collaboration, and increasing penalties, to the extent possible, for the criminals who commit payments fraud and scams; and
5. Continue to enhance and expand consumer education efforts.

External Collaboration

Payment fraud, in all its forms, represents crime perpetrated by criminals. EWS fully supports the entirety of all relevant stakeholders coming together as a team to do what they can to limit the ability of these nefarious actors from perpetrating these crimes. Regardless of which stakeholders are involved, it is the criminals that perpetrate these frauds that are the impetus of this problem. The fact that they are the ultimate source should be kept in mind at all stages of developing measures to protect consumers and stop fraudsters.

Determining who must be involved in detecting, preventing and mitigating fraud and scams is a critical, gating question. The payments and banking industries are obvious stakeholders, but many members—like Zelle and the financial institutions that offer it—are already taking a multitude of actions to combat scams and fraud. Looking upstream in a scam, the telecommunications, AI (artificial intelligence), social media, and online marketplaces are also essential contributors to any solution since most criminals perpetrate their scams through these channels. Oftentimes the reason a scam is successful is because the consumer receives a spoofed phone call or text, an AI-generated photo with message, or an advertisement or direct message on a social media platform from someone they purportedly trust. The criminals then build upon this trust through continued engagement with the consumer on these platforms, well before a financial transaction may even be initiated.

In these scenarios, EWS or a financial institution never sees the communication that leads to the consumer intentionally and voluntarily initiating a payment. Only the consumer knows whether they know and trust the person to whom they have decided to send money. By the time a consumer reaches the payment stage, they would need to be dissuaded from taking an action they have already decided to take, because their trust is with the criminals now. Attempting to stop the consumer at this stage carries its own dilemma because it is their money and it ultimately is, and should be, their decision whether to make any given payment with their money. In contrast, telecommunications, social media companies, and online marketplaces can combat criminals much earlier in the scam life cycle, before consumers have even been targeted. It is precisely because these criminals are taking advantage of the telecommunications', social media companies', and online marketplaces' platforms that uniquely position such industries to provide invaluable contributions in the fight against payments fraud and scams. Reducing the surface area of fraud and scams through engagement with telecommunications, social media companies, and online marketplaces is, therefore, essential.

Effectively addressing scams that originate on social media and online marketplaces will require proactive steps such as identifying and promptly removing both the fraudulent ads posted on these sites and the criminals behind those ads and accounts, as well as encouraging and acting on reported issues by consumers, other industries, and law enforcement. Additionally, insights from social media companies about how users are interacting with fraudulent ads, paired with information about the behaviors and actions of scammers operating on social media, would clarify how and where these crimes are proliferating. By bringing together data and information on what social media companies see with what customers report to their financial institutions, both sides could better identify bad actors, protect customers, and be nimbler in triaging emerging trends.

Additionally, enhanced collaboration with telecommunications companies should occur and include, at a minimum: (1) real-time alerts for suspicious account changes; (2) shared intelligence on compromised phone numbers; and (3) coordinated response to large-scale telecom fraud campaigns.

Collaboration should extend to email providers, social media platforms, and app stores, to (1) identify and eliminate fraudulent communications; (2) share threat intelligence on malicious

applications; and (3) coordinate takedown of fraudulent websites, phone numbers, and email addresses associated with fraud reports.

Soon, AI tools will be used more extensively by bad actors to deceive and build trust, making it important for the companies developing AI technologies to participate in scam reduction efforts. Specifically, AI companies must be able to provide information that makes it transparent to consumers that they are interacting with an AI-generated entity.

The government must also continue to play a role by enabling policy solutions and providing the resources needed to address the root causes of fraud and scams that impact the payments ecosystem upon which our economy and consumers rely. As a result, policy solutions to prevent fraud and scams must be directed at addressing fraud and scams where they actually exist including, for example, through criminals' use of social engineering and identity spoofing and across online marketplaces, mobile network operators, email, and social media platforms. The ultimate source of the problem is the fraudster who perpetrates fraud and scams and who, in the absence of being held accountable through criminal prosecution, will continue to victimize consumers. As such, a key aspect of policy solutions to address fraud and scams must be increased law enforcement and criminal penalties for the bad actors who perpetrate fraud and scams.

There should be enhanced collaboration with law enforcement and regulatory bodies, such as the Federal Bureau of Investigation (FBI), Department of Homeland Security (DHS), Secret Service, and state attorneys general, to: (1) provide rapid response to organized fraud campaigns; (2) share intelligence on criminal networks; and (3) coordinate prosecution strategies.

This government collaboration should extend to, and exist between, federal and state agencies. Developing a unified reporting system could allow institutions the ability to file a single report that all relevant agencies could access, which would reduce the reporting burden while improving access to key and unified information for the agencies. A permanent joint task force would combine regulatory expertise with law enforcement capabilities to address complex, multijurisdictional fraud schemes.

As already mentioned, the root of a fraud or scam payment is upstream of payment initiation by a consumer. Criminals initiate contact directly with a consumer and build trust using multiple communications channels over an extended period of time using highly targeted strategies based on the demographics of the intended victim. This is an opportunity for the banking regulators to work with the Federal Trade Commission (FTC), Federal Communications Commission (FCC), and Congress, if necessary, to facilitate enhancements to how social media and telecommunications companies combat payments fraud at its source. It is also an opportunity to involve prosecutors and other law enforcement agencies, in order to provide them with the information and resources needed to enhance their ability to investigate and prosecute the criminals who perpetrate fraud and scams – the ultimate source of these crimes.

While the above is a reasonable initial list of stakeholders at a high level, the task force called for by the recently introduced Task Force for Recognizing and Averting Payment Scams

(TRAPS) Act, in both the U.S. Senate and House, also presents a promising vehicle to ensure identification of a fulsome set of stakeholders, obtaining input from those stakeholders, and determining the best fraud mitigation and implementation strategies. The TRAPS Act would facilitate bringing together the public and private sectors with an interest and/or role in payments fraud mitigation and facilitate cross-sector collaboration to accomplish that goal. Given existing federal efforts to move toward electronic payments, such as the Executive Order *Modernizing Payments To and From America's Bank Account*, the task force the TRAPS Act envisions is especially timely.

In this vein, EWS also recommends creating a formalized, real-time fraud intelligence sharing network that enables participating institutions to share threat indicators, emerging fraud patterns, and a forum to share best practices. This network should: (1) provide legal safe harbors for information sharing under appropriate privacy protections; (2) operate 24/7 with automated threat intelligence distribution; (3) include standardized APIs for seamless integration with existing fraud systems; and (4) enable cross-payment rail visibility (ACH, wire, instant payments, cards, etc.).

Similarly, existing consortiums, like the National Task Force on Fraud and Scam Prevention, launched by the Aspen Institute Financial Security Program, could be replicated with leadership from the government and involvement from cross-sectional industry. Complex, multi-institution schemes require joint fraud investigation teams, shared blacklists and positive identification databases, coordinated response protocols for emerging threats; and regular cross-industry fraud simulation exercises. No single industry should (or could) be expected to resolve this in a vacuum. These are joint threats requiring joint solutions.

Once the correct actors are identified and frameworks are put in place, the question turns to the strategies to implement. We recommend placing a high priority on two strategies to combat payments fraud. The first is an increase to law enforcement funding and resources, and to coordinate a multijurisdictional response to increase criminal penalties for payments fraud. The root sources of payments fraud are the criminals that perpetrate it: dedicating resources to build expertise to identify a higher percentage of these criminals and subject them to more severe penalties is an effective measure to counter future payments fraud. We note, however, that holding the criminals accountable faces significant challenges given the cross-border criminal rings involved in these crimes.

The second high priority strategy focuses on real-time data sharing standards. Institutions have the capability of sharing fraud risk indicators as soon as they are detected and, with effective communication, can coordinate account freezes and transaction blocks across institutions. To work effectively and efficiently, institutions need consistent fraud classification methodologies, coordinated customer communication strategies, and a centralized data repository they can all access. One possible model is the Cybersecurity and Infrastructure Security Agency and the efforts made to develop a coordinated approach to cybersecurity.

Accomplishing the unified approach outlined above is not without obstacles. As institutions and agencies have worked to combat payments fraud in isolation, they have developed inconsistent data formats and classification systems. They also rely on differing

technology that may not allow for easy communication across institutions. Aside from these logistical hurdles, there is also regulatory uncertainty and privacy and compliance concerns around information sharing. Stakeholders may also have competitive concerns about sharing proprietary fraud detection methods. These obstacles should be taken seriously and are discussed further below.

Consumer, Business, and Industry Education

Because fraud and scams originate through fraudsters' direct engagement with consumers, well before a financial transaction is undertaken, it is imperative that policy solutions include reducing the number of criminal actors, as well as government sponsored consumer education so that consumers are armed with the information necessary to identify and avoid bad actors in the first place. Zelle and participating financial institutions on the Zelle Network provide consumers with a broad array of education resources to help them identify and avoid scams and safely navigate the payments landscape, including in-product messages and alerts presented to the consumer during the payment initiation flow, always-on consumer education campaigns, and direct engagements through branches and community workshops. Early and broad, nationwide engagement with consumers is key.

Through our work with several different groups, including the National Council on Aging, Consumer Action, and the Better Business Bureau, we have learned that delivering consumer education through community-based organizations that reach and are trusted by consumers allows for the message to resonate and help individuals the most. We have found success in the "train-the-trainer" model where we partner with a national organization to host fraud and scam trainings aimed at helping educate community-based organizations that work directly with the communities they serve.

Zelle provides access to the Zelle Pay It Safe Education Center on its website, which is designed to educate consumers on digital banking, fraud and scams, and how to stay safe when banking digitally. Zelle has also developed a consumer education video series that provides education on specific scams. These videos are displayed on the Zelle website, YouTube, and are made available for financial institutions in the Zelle network to use in their own channels.

Zelle stands ready to expand the reach of its many education initiatives through partnership with the government.

While consumer education is important, it is important to recognize it is not one-size fits all. Different audiences require different education because they tend to be susceptible to different kinds of fraud and scams. Consumers, for example, should be educated to recognize social engineering tactics, safe payment practices (like only using P2P with people and businesses you actually know), and recognition of scam advertisements and websites. Small businesses, on the other hand, are more vulnerable to compromised emails and scam vendors and should be better educated on prevention and verification in these areas. Financial institutions of all sizes should have more technical training on emerging fraud vectors and detection methods.

The most effective P2P fraud/scam education is delivered through multiple channels at the point of need, including:

- In-app notifications and warnings with interactive messaging;
- Security tips and information as part of online and banking apps, including contextual education based on transaction patterns;
- Peer-to-peer education through trusted community channels; and
- Entertaining and interactive learning experiences that engage users

A common problem with all scams, both those face to face and those in the digital age, is that consumers feel an artificial pressure to act quickly. Consumers are presented with a limited time to act and are not afforded an opportunity to pause and reflect on whether they are engaged with a scammer. Pop-up warnings and other real-time alerts during high-risk transactions allow consumers to take the pause that might stop them from completing a scam transaction.

As highlighted above, EWS and its participating financial institutions offer a plethora of consumer education, both integrated into the payment interfaces and outside of it. While these methods have proven extremely effective, cross-industry solutions would be even more successful. Social media platforms have a large megaphone that reaches an incredible number of consumers on a daily basis. They are uniquely positioned to contribute to the solution: indeed, the same trust consumers have when engaging on social media platforms that makes them more susceptible to criminals abusing those platforms can be utilized to spread consumer education and awareness. These companies should be encouraged to use their power and influence to educate consumers directly on payments fraud. They could also put in place notifications that mirror the in-app notifications Zelle and its participating financial institutions provide to help consumers pause and think in real-time before falling victim to payments fraudsters.

In addition to developing and adding new fraud education, existing education can be improved. To begin with, the messenger can enhance the strength of the consumer education message to incorporate the latest criminal tactics: there are numerous trusted messengers in consumers' lives available to update. These include but are not limited to: (1) financial institution customer service representatives; (2) community organizations; (3) high school and employer-sponsored financial education programs; and (4) peer networks. Existing and new fraud and scam prevention resources can be presented to consumers through these already trusted sources.

Community protection efforts could be broadcast and normalized as a form of "social proofing" such safety measures. Education tools could also take better advantage of loss aversion on the part of consumers by being explicit and detailed in presenting the consequences of falling victim to payments fraud.

Additionally, there should be a government-sponsored and private sector supported, centralized fraud education portal that is regularly updated and provides interactive fraud simulation tools. These tools would engage users and allow them to simulate the most common forms of scams to facilitate recognition when faced with those circumstances in the real world. The portal could offer personalized risk assessments that help consumers determine if they use safe payments practices and/or where they are vulnerable to being victimized or unwittingly

engaging in money mule activities. This portal should be mobile-optimized and offer multilingual content to ensure access to as many consumers as possible. Such a portal would be in stark contrast to the system in place today, comprising multiple agencies (*e.g.*, CFPB, FTC, USPIS, SS, and others) taking disjoined efforts to educate consumers with no clear collaboration. A national strategy and/or leader to direct and streamline these efforts would be more efficient and more effective.

Regulation and Supervision

While the current regulatory guidance is helpful, ideas for more detailed guidance include encouraging development and integration of real-time fraud monitoring capabilities, standardization of fraud detection system performance metrics, and customer notification standards for fraud prevention actions. Establishing detailed guidance would encourage standardization and help institutions coordinate fraud prevention efforts, including response times and information sharing protocols.

New guidance that prioritizes uniformity and information sharing can work toward creating a shared fraud prevention infrastructure that community banks and credit unions can access. This infrastructure can provide cloud-based fraud detection services, shared threat intelligence feeds, and standardized fraud prevention training programs that the community banks and credit unions would not have to invest in developing. The network should also provide technology implementation support because implementation would likely include technology not currently present at all financial institutions.

Smaller financial institutions could be offered the opportunity to participate in the collaborative fraud prevention program without being asked to make as significant of contributions. Options would include, for example, reducing individual reporting requirements when participating in industry-wide initiatives.

Regarding the regulation of checks and the continued problem of check fraud specifically, EWS notes that the best solution to check fraud is the continued decreased reliance on checks. The current administration agrees—Executive Order 14247, "Modernizing Payments to and from America's Bank Account"—goes into effect September 30, 2025, and requires the U.S. Treasury to stop issuing paper checks for most federal payments, in favor of electronic payment methods. While Zelle should only be used for transfers to persons and businesses known to the transferee, under those circumstances Zelle is simply a safer and more efficient method to accomplish the same goal as paper checks. Indeed, Zelle was designed to provide consumers with greater access to, and utility for, their bank deposit accounts by providing an innovative digital means of sending and receiving money as an alternative to checks and cash. Unlike checks, funds transfer using Zelle without having to share sensitive financial information, such as bank account or routing numbers, and the digital nature of Zelle allows for integration of comprehensive fraud and scam prevention strategies, such as Zelle's recipient name matching capability that requires the sender to confirm the expected recipient's first name. Checks have a physical form that can be intercepted by bad actors and manipulated. The more transactions in

which checks can be replaced by more secure payment methods like Zelle, the less check fraud.

Payments Fraud Data Collection and Information Sharing

Payments fraud data collection and information sharing could be improved by creating a standardized industry data repository that (1) uses consistent fraud classification systems (building on FraudClassifier and ScamClassifier models); (2) provides real-time data sharing capabilities; (3) maintains appropriate privacy protections; and (4) enables cross-payment rail analytics.

Data collection and information sharing could also be enhanced by implementing automated data collection systems to capture fraud attempts in real-time and standardize data formats across institutions. This would both reduce the reporting burden on financial institutions and enable rapid threat identification and response.

The fraud data elements to collect include real-time transaction risk scores, customer behavioral analytics, device and channel intelligence, social engineering indicators, and cross-institution relationship mapping. These data elements are obtainable from payment processors and networks, financial institutions, telecommunications providers, technology companies, and law enforcement agencies.

There are numerous barriers to overcome to accomplish these data sharing goals. First are the logistical challenges: today different stakeholders have varied data formats and definitions and any attempt to create a unified system will undoubtedly face technological integration challenges. Apart from the logistics, there are also privacy and compliance concerns, hesitations with sharing proprietary information, and overall regulatory uncertainty about what they are allowed to share and under what circumstances. The regulatory challenges, privacy, and compliance concerns may be alleviated with regulatory safe harbors for fraud and scam prevention sharing. Any competitive concerns may require industry-standard data sharing agreements. To solve the logistical concerns, there will need to be standardized APIs for data exchange.

The FraudClassifier and ScamClassifier models are excellent models but need certain improvements. They should be expanded to cover emerging fraud types. They should be integrated with real-time transaction monitoring systems and equipped with predictive analytic capabilities. As with every other suggestion herein, the key will be standards: there should be standardized implementation guidelines. Federal agencies play an important role in combating payments fraud. They should encourage industry-wide adoption by the payment networks of the standardized models described above. They can provide technical assistance as stakeholders implement these standardized models and can establish performance metrics and benchmarks to assist with adoption and validation. They can also coordinate with international standard-setting bodies.

A fraud management lesson learned from card networks is to send as much contextual information as possible with a transaction for a better payment authorization decision by the card issuer. Information such as merchant category code and use case (quasi-cash, card not present,

etc.) are used in card rules and machine learning models prior to approving a payment. Unfortunately, the same level of data is not available in payments like wires and ACH. Appropriately tagging payment transactions with contextual data can help in the detection of fraud and scam transactions.

In addition to these models, a centralized database for the sharing of payments fraud data across entities, analogous to the 314(b) information-sharing program adopted in response to money laundering threats established by FinCEN, would be a significant difference maker in combatting payments fraud. EWS has developed such a repository—The National Shared Database. It contains a broad set of deposit performance and transaction history data used by participating institutions to make informed decisions about account applications, payments, and other transactions. This database provides a myriad of benefits. However, unlike with 314(b), GLBA does not provide a safe harbor for the sharing of information for frauds and scams. EWS encourages the financial regulators to work with Congress to secure a statutory safe harbor, and in the intervening time, issue guidance supporting such information sharing.

The benefits of a centralized database are that it provides comprehensive fraud visibility across payment rails and assists with rapid threat identification and response. It further helps coordinate industry defense strategies and allows stakeholders to take advantage of enhanced analytics and pattern recognition.

The challenges with developing and maintaining such a database are primarily those already identified above—privacy, regulatory compliance, competition, and technological integration issues. We add that centralizing information increases the target for cyberattacks and the risks associated with a successful cyberattack.

Reserve Banks' Operator Tools and Services

The key is increasing standardization and information sharing. Fraud reporting requirements should be extended to all payment rails operated by Reserve Banks which should implement real-time reporting capabilities. Reserve Banks should also standardize fraud classification systems and develop cross-payment rail analytics. Likewise, Reserve Banks should incorporate automated threat detection and alerting. Standards for fraud prevention should include minimum required fraud detection capabilities and uniform fraud investigation procedures. It would be further helpful to have developed performance metrics and benchmarks for participating financial institutions to meet.

In addition to these improvements on existing risk management tools, the Reserve Banks should work with existing fraud contact directory providers to ensure there is a secure, real-time fraud contact repository. This directory should provide 24/7 contact information for fraud teams, enable rapid communication during fraud events, and include escalation procedures for more complex cases. It should maintain current contact information through automated updates.

Notification systems can rely on machine learning to identify unusual patterns. Real-time alerts to relevant institutions and recommended response actions will help ensure timeliness and

consistency in responses. The contact directory and notification systems combine to enable coordinated responses to emerging threats.

Steps can also be taken in the payments system itself. For example, confirmation of payee services should be developed that will verify recipient identity before payment completion and provide real-time account verification. Other potential improvements include risk scoring based on recipient history and enabling sender education about potential risks of sending before any transaction completes.

General Questions

Putting aside check fraud, which remains a concerning type of fraud and why we strongly recommend exploring every opportunity to lower the usage of checks, the most widespread fraud types are social engineering attacks that can result in account takeover fraud or impersonation scams. The former is when the attack induces the consumer to provide credentials into their banking account. Account takeover fraud has included credential stuffing attacks using stolen data, SIM swap attacks targeting mobile authentication, and malware-based account compromise. Impersonation scams are when criminals posing as trusted individuals or organizations— banks, government agencies, businesses, friends, family, etc.—induce the consumer to provide sensitive information through deception or manipulation. Examples include romance scams, business email compromise affecting commercial customers, tech-support scams exploiting trust in authority, and impersonation fraud leveraging public information.

EWS employs a multi-layered approach to combat fraud and scams, including consumer education, fraud monitoring, messages and confirmations during payment flow, and the use of real-time monitoring services. EWS has developed a first of its kind proprietary service unique to the Zelle network called Risk Insights for Zelle ("RIZ") that provides real-time risk attributes regarding recipients to participating financial institutions before the institution initiates a transfer. Under the Zelle network rules, participating financial institutions must use RIZ data to evaluate risky transactions to determine whether to stop or delay them in real-time. RIZ data elements include, for example, how long a particular token has been registered, how many users sent payments to the token recently, total dollar amounts sent to the token recently, and other factors that may be helpful to a financial institution evaluating the risk of a transaction using its risk engine. RIZ is dynamic so that EWS can update the data elements as fraudsters evolve their tactics.

EWS's onboarding fraud control requirements work to keep bad actors off the network in the first place. All Zelle users must have a depository account at a U.S. financial institution to enroll in Zelle, ensuring the user is protected by the financial institution's highly regulated account opening process, including BSA/AML and KYC obligations. In addition to regulatory account opening protections, the Zelle network rules require participating financial institutions to use multiple authentication tools to validate users' Zelle tokens, including measures like one-time-passcodes sent to a user's mobile phone to confirm possession of the phone when users enroll in Zelle. Participating financial institutions are also required to ensure that: (1) phone

numbers used as tokens are valid, active, and assigned by a mobile network operator identifying the user as an authorized user; (2) the same user has control and possession of the phone number; and (3) the mobile phone number is associated with a U.S. mobile network operator and is not an international number. Similar requirements exist for email addresses, with the addition that EWS prevents enrollment of email tokens that contain a potentially misleading word, phrase, or email domain. Each of these features make it harder for fraudsters and scammers to obtain access to the Zelle network in the first instance.

Users receive real-time notifications, warnings and reminders when enrolling in or using Zelle. During the initial enrollment process, users must review the Zelle terms and conditions of their financial institution, which include a prominent notice that Zelle is intended to send money to friends, family, and others you trust – not to recipients you are not familiar with or do not trust. The Zelle network rules also require all participating financial institutions to provide real-time warnings and notifications to users before sending transfers. The user must select from their contact list or enter the unique token of the receiving party to whom they seek to send funds and, before the transaction is completed, EWS provides the sending bank with real-time data attributes to conduct a risk analysis before allowing the transfer to occur. The user is given several opportunities to verify the recipient is correct. These include requests to confirm the token of the recipient, confirm that the first name of the recipient (provided by Zelle based on the token entered) matches the user's expectation, and reminders not to send money using Zelle to people they do not actually know and that payments cannot be canceled once confirmed. Only after receiving all these notifications, warnings, and reminders, can the user choose to proceed with the payment.

EWS also mandates fraud and scam reporting and blocking to identify and exclude bad actors. Participating financial institutions are required to report suspected fraud or scams to EWS no later than one business day after notification by users. EWS notifies the recipient's participating financial institution, which must investigate and respond within five business days. The recipient's financial institution may take action to restrict their customer from the Zelle Network and/or close their customer's deposit account. Following independent reports that a recipient has engaged in a suspected fraud or scam, EWS will itself restrict the suspected bad actor's token from the Zelle Network (if a participating financial institution has not already done so). In addition, EWS has a system in place for most consumer accounts to restrict all tokens associated with the suspected bad actor at any financial institution through which the bad actor is enrolled or seeks to enroll in Zelle as well as restrict that actor's customer identification at that financial institution, thereby preventing the actor from enrolling in or accessing Zelle.

EWS and participating financial institutions have also been heavily involved in educating consumers about payments fraud, examples of which are provided above. One of the most critical tools has been contextual fraud warnings during transactions. Scams necessarily require convincing the consumer to take a risky action and clear and conspicuous fraud warnings during the payments process is the most effective means of dissuading them. EWS and its participating financial institutions also rely on proactive customer communications about emerging threats and community-based fraud awareness programs so consumers will recognize payments fraud

attempts and proactively take preventative measures, as well as fraud prevention training for customer-facing staff so that staff are equipped to assist consumers efficiently and effectively when these issues arise.

Consumers assist in combatting payments fraud through proactive communication about unusual activity and immediately reporting suspicious communications. These consumer reports are one of several data points used to identify and potentially limit suspicious accounts and transactions. Consumers also benefit by participating in fraud prevention education, as more educated consumers are less vulnerable to scams and more secure use of payments systems are less vulnerable to fraud. One valuable action consumers can take is to move away from less secure options, like checks, to more secure options.

Consumer education is the best way to encourage the use of secure payment methods by making customer aware of the benefits of these methods. There should be clear communication about the security features at issue and their practical benefits as opposed to the comparatively weaker security for other payment methods. This would naturally fit within fraud prevention best practices education, which would likely highlight the higher risks associated with less secure payment methods. Education can also showcase success stories of these security benefits in action.

Conclusion

Early Warning Services believes that addressing payments fraud requires a whole-of-society, collaborative approach that balances innovation with security. The recommendations outlined in this response emphasize the importance of real-time information sharing, standardized processes, and industry-wide cooperation in building a more secure payments ecosystem.

We stand ready to work with the Federal Reserve, FDIC, OCC, and other agencies to implement these recommendations and continue advancing the security and integrity of the U.S. payments system. Our experience operating the Zelle network and providing fraud prevention solutions positions us to contribute meaningfully to these critical efforts.

We appreciate the opportunity to take part in this important dialogue and look forward to continued collaboration in addressing the evolving challenges of payments fraud.

Respectfully submitted,

Ben Chance
Early Warning Services, LLC's
General Manager of Identity and Payments
Risk Business