Statement of

Cameron Fowler
Chief Executive Officer, Early Warning Services, LLC

Permanent Subcommittee on Investigations
Committee on Homeland Security and Governmental Affairs
United States Senate

July 23, 2024

Chairman Blumenthal, Ranking Member Johnson, and distinguished Members of the Subcommittee, thank you for the opportunity to testify today regarding the Zelle Network®. I have the privilege of serving as Chief Executive Officer of Early Warning Services, LLC ("Early Warning" or "EWS"), which operates the Zelle Network.

Early Warning's 30-Year History of Success Protecting Consumers and the U.S. Financial System

Early Warning has been empowering and protecting consumers, businesses, and the U.S. financial system with cutting-edge fraud prevention and payment solutions for more than three decades. Early Warning works with more than 3,500 banks, credit unions, businesses, and the U.S. government to increase access to, and protect, the financial system and the consumers who rely upon it. For example, in 2023 alone, EWS helped financial institutions screen $10.4 trillion in transactions and stop $2.8 billion in potential fraud. In light of EWS's proven success in enabling payments and combatting fraud, EWS's owner banks engaged EWS to develop and operate the Zelle Network. Zelle® is an innovative digital alternative to checks and cash designed to provide consumers with greater access to, and utility for, their insured deposit accounts at regulated financial institutions. Zelle enables U.S. financial institutions of all sizes to provide their customers with the ability to quickly send money to friends, family, and others they know and trust.

The Innovative Design of Zelle Democratizes Payments For Consumers, Community Banks, and Credit Unions

In 2023, 120 million consumers and small businesses made everyday transactions with Zelle. For example, friends and family members use Zelle to send money to one another and others whom they know and trust. Additionally, insurance companies and charitable organizations turn to Zelle to quickly disburse funds to victims of disasters and to those in need. Participating financial institutions generally provide Zelle to their customers as a value-added service without fees.

Users make peer-to-peer ("P2P") payments with Zelle either through their participating U.S. domestic financial institution's secure online banking website or mobile banking application. Local community banks and credit unions, who are often the financial mainstay of

rural, minority, and low-to-moderate income communities, rely on Zelle as the P2P solution of choice to serve their customers' needs. In fact, 95% of the financial institutions participating in the Zelle Network are community banks and credit unions. This includes nearly 50% of Minority Depository Institution (MDI) banks. If not for Zelle these small banks and credit unions may not otherwise be able to offer this valuable P2P service to the communities they serve.

Zelle Provides Best-in-Class Consumer Protection

EWS remains steadfastly committed to protecting Zelle users from fraud and scams through an extensive array of highly effective fraud and scam countermeasures. The Zelle Network's commitment to consumer protection is reflected in its demonstrated record of success: over 99.9% of all Zelle transactions are completed without any report of fraud or scam. Indeed, from 2022 to 2023 reports of fraud and scam payments processed on the Zelle Network decreased – while we simultaneously grew our network and increased transaction volume.

For nearly two decades, EWS has been subject to extensive regulatory oversight and supervision by both the Office of the Comptroller of the Currency ("OCC"), and subsequently, the Consumer Financial Protection Bureau ("CFPB"). In addition, all financial institutions that participate on the Zelle Network are chartered, insured, regulated, and supervised under U.S. banking laws – a requirement to participate in the Zelle Network.

Financial institutions participating in the Zelle Network are governed by the Zelle Network Participation Rules ("Zelle Rules"). The Zelle Rules are maintained and enforced by EWS, and all participating financial institutions must agree to abide by these rules to participate in the Zelle Network. EWS continuously monitors and takes appropriate action to ensure compliance with all requirements, including those applicable to consumer protection and the detection and prevention of fraud and scams.

Safety and security are core tenets of the Zelle Network's design. As an initial matter, Zelle payments are sent directly between U.S. domestic chartered and regulated financial institutions, a design feature unique to Zelle. All Zelle transactions are made from one insured deposit account to another without users having to share sensitive account or personal information. In operating the Zelle Network, EWS does not hold funds nor manage custodial accounts; rather, all funds are maintained by and transferred directly from and to the consumer's existing bank or credit union account and settled directly by and between financial institutions. Consumers are provided Zelle as a value-added service for their deposit accounts, and payments are made available typically within minutes, meaning customers do not have to wait several days or pay a fee to access funds in their bank account. This provides consumers timely access to funds when they need them while helping them to better manage their money.

Zelle requires all participating financial institutions to use authentication and enrollment controls, which may include (but are not limited to), usernames, passwords, biometric data, encrypted identity verification data, real-time monitoring of enrollment tokens, and data-driven technology for real-time identification of potential bad actors allowing financial institutions to interdict and stop potentially high-risk transactions.

EWS and participating financial institutions in the Zelle Network educate consumers about the evolving risks of fraud and scams to help protect themselves, including in-app safety messages and alerts presented to the consumer during the payment initiation flow, as well as broad-based consumer education campaigns that have reached tens of millions of consumers; including campaigns that are tailored to older Americans, college-aged students, servicemembers, veterans, and other groups. Users encounter various warnings at enrollment and continuously through real-time alerts displayed throughout the payment process. These warnings include a Safe Use Alert, which reminds users before they are able to complete a transaction that they should only use Zelle to pay people they know and trust, alerting users to be on the lookout for scams, and that payments may not be reversible or recoverable. The in-app notifications also include a recipient name alert that displays the user's legal first name as verified by the financial institution at account opening (not a "handle" or username created by the user) under Know Your Customer ("KYC") requirements in the Bank Secrecy Act. These are provided to the sending user to assist in verifying the recipient.

Given the dynamic and increasingly sophisticated nature of the tactics employed by criminals, EWS is also constantly innovating and evolving its consumer protection fraud and scam countermeasures.

Zelle Provides Industry-Leading Reimbursement Benefits

The Zelle Rules go further than the requirements of the Electronic Fund Transfer Act ("EFTA") and Regulation E, and require all participating financial institutions to provide full reimbursement for Zelle transactions determined to be unauthorized under the EFTA and Regulation E, even when the consumer would otherwise be liable for some portion of the payment under the law. Financial institutions in the Zelle Network are required to fully reimburse customers for fraudulent transfers – that is transfers that were unauthorized, going above what the law requires. Additionally, Zelle goes well beyond existing legal requirements and requires reimbursements for the victims of qualifying imposter scams where the consumer was duped into sending money to a criminal posing as a government agency, financial institution, or service provider.

EWS takes reports of fraud and scams seriously. EWS refers consumers to their participating financial institutions to investigate reports of fraud and scams because financial institutions are in the best position to assist their customers given these institutions maintain their customers' accounts, related account information, and transfer the funds.

Zelle Welcomes the Opportunity to Partner with Congress to Advance Policy Solutions to Prevent Fraud and Scams

Fraud and scams typically occur prior to, and separate from, the means of money transfer, and outside the purview of the relevant payment network, including the Zelle Network and participating financial institutions. Typically, criminals engage consumers through social media, emails, or identity spoofing – not through Zelle. Although Zelle and its participating financial

institutions provide industry-leading consumer protection measures, we cannot single-handedly prevent all acts of criminals who defraud both consumers and financial institutions.

Government also has a critical role to play by enabling much needed policy solutions and providing the resources required to address the root causes of financial fraud and scams that impact the payments ecosystem upon which our economy and consumers rely. Policy solutions to prevent fraud and scams must be directed at addressing fraud and scams where they originate including, for example, across online marketplaces, mobile telecommunications networks, email, and social media platforms. The ultimate source of the problem is the criminal who perpetrates the fraud and scams and who, in the absence of being held accountable through criminal prosecution, will not be deterred from continuing to victimize consumers. As such, a key aspect of policy solutions to address fraud and scams must be increased law enforcement and penalties for the criminals who perpetrate fraud and scams. Furthermore, because fraud and scams typically originate through criminals' direct engagement with consumers, it is imperative that policy solutions include government-sponsored consumer education so that consumers can more easily spot scams and avoid engaging with criminals. Zelle and participating financial institutions already provide consumers with a broad array of education resources to help them identify and avoid scams and safely navigate the payments landscape. We welcome the opportunity to partner with government agencies to expand the reach of these efforts.

Toward that end, we urge Congress to enable the following policy solutions to combat fraud and scams and protect consumers:

- Leverage government resources to better educate consumers about common frauds and scams;
- Increase law enforcement resources needed to prosecute fraudsters and ensure the sentences for consumer fraud are effective deterrents;
- Stop bad actors from spoofing their identities on phone calls by requiring mobile network operators to fully block spoofed calls; and
- Improve identity verification to stop bad actors from accessing the financial system by providing financial institutions with free access to the Social Security Administration's Electronic Consent-Based Social Security Number Verification ("eCBSV") system.[1]

In addition, EWS fully endorses the proposal set forth in the Senate Appropriations Committee's FY24 Financial Services and General Government bill report, which directs the Treasury Department to lead a multisectoral whole-of-society effort to counter the increasing threats associated with financial fraud. EWS supports the creation of public-private partnerships between government and private sector participants to facilitate collaboration, sharing of best

[1] The eCBSV system helps keep bad actors out of the financial system by performing a simple background check; an institution using eCBSV submits a potential customer's name, date of birth, and social security number, and eCBSV indicates whether the data provided match the Social Security Administration's internal records.

practices, and the development of innovations in counter-fraud technologies, data analytics, and other approaches to combat fraud and scams.[2]

Building upon this effort, Early Warning organized leaders across multiple industries, along with government agencies and experts, as part of a National Task Force for Fraud & Scam Prevention to develop recommendations for broader strategies to combat fraud and scams. This cross-industry partnership will launch with a summit this fall where the group will focus on three key areas:

- **Consumer education**: Educating consumers on how to spot and report scams through a broad-based public education campaign.
- **Fraud and scams prevention and detection**: Scaling up intelligence and best practices sharing across sectors on the latest scams and tactics.
- **Recovery and prosecution:** Identifying and prosecuting fraudsters and scammers.

We welcome the opportunity to work with this Subcommittee as well as other members of Congress to further identify and develop meaningful legislative solutions directed at protecting consumers while preserving the benefits of Zelle and real-time payments, which millions of consumers reliably utilize without issue.

Thank you for the opportunity to testify today. I look forward to your questions.

[2] Financial Services and General Government Appropriations Bill, S. Report 118-61, at 10 (2023), *available at https://www.congress.gov/congressional-report/118th-congress/senate-report/61/1*.