EXHIBIT A

SUPREME COURT OF THE STATE OF NEW YORK
COUNTY OF NEW YORK

PEOPLE OF THE STATE OF NEW YORK, by LETITIA JAMES, Attorney General of the State of New York, Plaintiff, v. EARLY WARNING SERVICES, LLC, Defendant.	Index No. 654753/2025 IAS Part 35 Hon. Phaedra F. Perry-Bond

[PROPOSED] BRIEF OF *AMICI CURIAE* AMERICAN BANKERS ASSOCIATION, BANK POLICY INSTITUTE, CONSUMER BANKERS ASSOCIATION, INDEPENDENT COMMUNITY BANKERS OF AMERICA, NATIONAL BANKERS ASSOCIATION, AND NEW YORK BANKERS ASSOCIATION IN SUPPORT OF DEFENDANT'S MOTION TO DISMISS

MANATT, PHELPS & PHILLIPS, LLP
7 Times Square
New York, New York 10036
(212) 790-4500

GLASER WEIL FINK HOWARD JORDAN & SHAPIRO, LLP
10250 Constellation Blvd., 19th Floor
Los Angeles, California 90067
(310) 556-7880

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES & RULES

OTHER AUTHORITIES

STATEMENT OF INTEREST OF *AMICI CURIAE*

This brief is filed on behalf of national and New York State banking trade organizations (collectively, the "*Amici*"), each of which includes members that formally participate in the Zelle network and otherwise engage in financial transactions involving competitor peer-to-peer payment applications such as Venmo, PayPal and Cash App, among others. A complete description of the trade associations and their roles is set forth in the accompanying affirmation of Richard E. Gottlieb. The trade associations are as follows: American Bankers Association, Bank Policy Institute, Community Bankers Association, Independent Community Bankers of America, National Bankers Association, and the New York Bankers Association.[1] *Amici* believe this proposed amicus curiae brief would help the Court.

Amici respectfully submit this memorandum of law to explain how the New York State Attorney General's ("NYAG") unprecedented attempt to hold EWS liable under state law for the fraudulent conduct of bad actors who induce customers to authorize payments within the Zelle network would incentivize scammers, thereby negatively impacting the millions of bank customers who rely on Zelle for fast, secure, and reliable electronic payments, as well as the banks that support that process. Given that the listed trade associations represent both Zelle members and banks outside the network, *Amici* can offer arguments that might otherwise escape the Court's consideration.

[1] Seven of the largest banks collectively own Early Warning Services, LLC ("EWS"): Bank of America, Capital One, JPMorgan Chase, PNC Bank, Truist, U.S. Bank, and Wells Fargo. *See* Consumer Fin. Prot. Bureau, Early Warning Services, LLC, https://www.consumerfinance.gov/consumer-tools/credit-reports-and-scores/consumer-reporting-companies/companies-list/early-warning-services-llc/ (last visited Apr. 29, 2026). Along with thousands of other financial institutions, these seven banks are also members of most (but not all) of the listed trade associations.

INTRODUCTION

Over the last several years, peer-to-peer payment applications ("P2P payment apps") have brought substantial benefits to consumers' ability to receive and send money efficiently and safely. Every day, millions of Americans use P2P payment apps like PayPal, Venmo, Cash App, and Zelle, among others, to make payments conveniently and without the inherent risks associated with carrying large amounts of cash or the loss or theft of personal checks and money orders. Consumers rely on these services to conveniently make numerous routine payments, such as paying household service providers, family and friends, and rent and other bills.

This lawsuit targets Zelle's operator, EWS. Thousands of financial institutions participate in the Zelle network, ranging from the largest national banks to local community banks and credit unions. As a result, Zelle payments and the Zelle payment network are widely accessible to consumers with a bank account in New York and across the country.

As shown below, Zelle payments are nearly incident-free—99.9% of payments occur without a *claim* that a fraud or scam occurred, let alone confirmed fraud.[2] That is no accident: the financial institutions that participate in Zelle do so because EWS employs numerous security measures to ensure that sensitive account details remain private and each payment reaches its intended recipient. These measures include not only technological precautions but also warnings to consumers explaining how scammers exploit victims, encouraging users to be vigilant, and cautioning them only to send money to people they know and trust.[3] For example, warnings are displayed when a user adds a new contact. Warnings are also displayed and must be acknowledged

[2] Zelle, *The Facts About Zelle and Scams*, https://www.zelle.com/sites/default/files/2026-01/Zelle-Fact-Sheet-Zelle-and-Scams.pdf (last visited Apr. 29, 2026).

[3] *Id.*

by the customer before a funds transfer. This includes pop-up warnings in large print that encourage the user to check the recipient of the proposed transfer.

Participating banks already reimburse customers when their accounts are hacked. The NYAG does not allege that participating institutions have failed to honor their commitments to reimburse for losses due to hacking under applicable law. Rather, the NYAG claims EWS did not sufficiently protect customers from third-party scams (so-called "induced fraud")—situations where an accountholder knowingly and voluntarily makes a payment to a third-party wrongdoer acting under false pretenses, almost always through false advertisements or communications on commercial platforms *outside* the Zelle network. (*See* Compl. ¶ 45). The NYAG accuses EWS of fraud because it failed to detect and prevent these scams. (*Id.*). And the NYAG seeks to have this Court require EWS to adopt broad—but also vague and undefined—"antifraud measures" that could only be implemented *nationwide* given the nature of the Zelle Network and the hundreds of millions of interstate payments implicated here.

Amici share the NYAG's concern about the pervasiveness of financial fraud and scams. New Yorkers (and all Americans) are under constant attack from bad actors who attempt to trick consumers into sending money to those wrongdoers. But leaving aside the multiple legal reasons why the suit is improper, it would be bad public policy to permit this lawsuit to proceed. The NYAG's efforts to prescribe far-reaching and substantive scam-prevention requirements, effectively nationwide, through a general New York anti-fraud statute, will only increase costs, decrease access to financial services, and hamstring EWS's (and participating banks') efforts to combat scams in an ever-evolving landscape. Indeed, the remedies sought by the NYAG would:

1. ***Reduce the consumer incentive to remain vigilant for scams, thereby emboldening fraudsters because consumers will be reimbursed no matter the circumstances.*** Others might take advantage of blanket reimbursement by submitting false scam claims.

2. ***Impose an impossible burden on EWS to both prevent and insure against customer-authorized transfer of funds over the network***. Like other P2P payment apps, Zelle allows consumers to send money according to the consumer's directions to the network. Technological "antifraud measures" will not alleviate what is ultimately a problem of human psychology and social manipulation by sophisticated bad actors. EWS and the participating banks see only the execution of a payment, not the intent behind it. While combatting scams remain a major focus of the financial industry, EWS and the Zelle participating institutions cannot prevent or insure against misconduct occurring *outside* the Zelle Network that induces a consumer to authorize payment to a bad actor via Zelle.

3. ***Make Zelle less accessible for consumers because the cost of customer reimbursement for scams would ultimately be passed on to consumers***. Smaller financial institutions (such as community banks and credit unions), especially those with more limited resources, may not be able to incur the cost of reimbursing for all scams, which could cause them to pull out of the Zelle network entirely or start charging a fee for each transfer. That would reduce network availability and limit access to a critical financial service (and the only one provided entirely through insured depository institutions), driving users to potentially less secure platforms.

Amici appreciate that, by this action, the NYAG is seeking to protect consumers and to fight fraud. But, rather than reducing scams, the NYAG's suit inadvertently incentivizes *more* misconduct and creates greater risks, harming the very consumers the NYAG seeks to protect. By any fair reading, N.Y. Exec. Law § 63(12) ("Section 63(12)") does not support the sweeping

liability the NYAG seeks to impose here, and *Amici* believe it should not be misused to this counterproductive end. Accordingly, *Amici* respectfully contend that dismissal of the NYAG's claims here is warranted.

ARGUMENT

I. EWS employs robust security measures that the NYAG claims undermine, not support.

As with other major P2P payment apps, Zelle is a critical part of the economy. Accordingly, this case has significant implications for millions of consumers across New York and nationwide. Individuals and small businesses rely on the ability to send and receive payments quickly and securely through these electronic payment platforms. Zelle meets that need by providing a secure, widely accessible P2P payment service.

Zelle operates through a network of more than 2,300 participating financial institutions of all sizes, from large national banks to local community banks and credit unions, including many in New York. Zelle is integrated in and directly accessed through the secure mobile banking apps and online banking sites of participating institutions, making access easy and convenient for account holders.[4] Zelle charges nothing for its services.[5] When both parties to a transaction are enrolled in Zelle, payment typically processes right away.[6] Because Zelle transfers funds directly between bank accounts, the money remains in FDIC-insured accounts before and after the

[4] Zelle, *Zelle Reaches Five-Year Milestone with More than Five Billion Safe, Secure Transactions* (Sept. 8, 2022), https://www.zelle.com/press-releases/zelle-reaches-five-year-milestone-more-five-billion-safe-secure-transactions (last visited Apr. 29, 2026); *see also* Zelle, *Zelle Fast Facts: History, Data Points and Common Questions* https://www.zelle.com/data-center (last visited Apr. 29, 2026).
[5] *See* Zelle, *Are There Any Fees to Send Money Using Zelle?*, https://www.zelle.com/faq/are-there-any-fees-send-money-using-zelle (last visited Apr. 29, 2026).
[6] Zelle, *How Long Does It Take to Receive Money with Zelle?*, https://www.zelle.com/faq/how-long-does-it-take-receive-money-zelle (last visited Apr. 29, 2026).

transfer.[7] Critically, all of these features—which are unique to Zelle—collectively make its service fast, secure, and easy to use.

Since its launch in 2017, Zelle has become one of the most relied-upon P2P payment apps platforms.[8] In 2025, U.S. individuals and small businesses sent more than $1.2 trillion using Zelle through 4.2 billion total transactions.[9] Individuals routinely rely on Zelle throughout their daily lives—to split the check at a restaurant, to pay for rent or childcare, or to send money to a friend or family member in need. And millions of small businesses across the country—contractors, caregivers, manicurists, landscapers—depend on Zelle.[10]

A significant security feature of Zelle is that EWS operates the application nationwide using uniform Network Rules.[11] As a result, granting the relief the NYAG seeks would change how Zelle works for all Americans by forcing changes to the Network Rules that could only occur nationwide.

The popularity of Zelle stems from the utility and accessibility it offers to consumers and small businesses alike. Zelle reduces consumers' need to carry cash, which itself presents risk, or to write checks, a top target for fraudsters. Instead, consumers can send and receive funds quickly,

---

[7] *See* Blankinship & Foster, *Zelle vs. Venmo: Which Is Better?*, https://www.bfadvisors.com/zelle-vs-venmo-which-is-better/ (last visited Apr. 29, 2026).

[8] Zelle, Zelle Posts 20% Growth with $1.2 Trillion Sent, Far Outpacing Consumer Spending and Cementing Its Role in the U.S. Economy (Feb. 11, 2026), https://www.zelle.com/press-releases/zelle-posts-20-growth-12-trillion-sent-far-outpacing-consumer-spending-and-cementing (last visited Apr. 29, 2026).

[9] *Id.*

[10] *Id.*

[11] Early Warning Services, LLC, *Zelle: Bringing Together Community Financial Institutions and Consumers to Help Prevent P2P Payment Fraud and Scams*, at 13, https://www.earlywarning.com/sites/default/files/2025-01/Zelle%20eBook%20%20Community%20Approach%20to%20Fraud%20and%20Scam%20Prevention.pdf (last visited Apr. 29, 2026)

without having to pay an "instant access" fee. And, with Zelle, all funds are debited from and credited to FDIC-insured bank accounts.[12]

For small businesses, Zelle eliminates the need for complex, costly payment solutions with third-party intermediaries such as payment processors.[13] A vendor can seamlessly take electronic payment without a point-of-sale system—that payment lands right into the vendor's bank account at a trusted financial institution, with no delays or issues caused by intermediaries.[14] Zelle lessens a small business's need to carry cash and can help reduce reliance on checks, thereby reducing the problem of bad checks (and delays caused by waiting on checks to clear).

A. Despite the NYAG's concerns, the EWS safety record shows it employs robust, proactive, and constantly evolving safeguards.

Amici appreciate the concerns expressed by the State of New York, and its members are actively involved daily in attempting to diminish these risks. However, despite the allegations in the NYAG's Complaint, the overwhelming majority of payments made using Zelle—99.98% as of last year—happen without any reports of suspected fraud or scam activity.[15] And that has been consistently true over the years: 99.9% of the five billion transactions on Zelle between 2017 and 2022 happened without any reports of scams or frauds, let alone a confirmed incident.[16]

---

[12] Blankinship & Foster, *Zelle vs. Venmo*, *supra*.
[13] *See* Early Warning Services, LLC, *Deep Dive Data Drop: Zelle® Unveils First-Ever Small Business Report—Here's What It Reveals* (Apr. 28, 2025), https://www.earlywarning.com/press-release/deep-dive-data-drop-zeller-unveils-first-ever-small-business-report-heres-what-it (last visited Apr. 29, 2026).
[14] *Id.*
[15] Zelle, *Zelle Hits New Highs: Two Billion Transactions and Nearly $600 Billion in Payments in First Half of 2025* (Sept. 16, 2025), https://www.zelle.com/press-releases/zelle-hits-new-highs-two-billion-transactions-and-nearly-600-billion-payments-first (last visited Apr. 29, 2026).
[16] Consumer Bankers Ass'n, *CBA, Leading Financial Groups Respond to Senator Warren's Report on Zelle* (Oct. 2, 2022), https://consumerbankers.com/press-release/cba-leading-financial-groups-respond-to-senator-warrens-report-on-zelle/ (last visited Apr. 29, 2026).

EWS and the institutions participating in Zelle employ robust and highly effective security measures. Those measures currently include using end-to-end encryption to send username, password, or biometric data to the financial institution to confirm users' identities; requiring users to have a U.S. mobile phone number and email address and a U.S.-based bank account with a regulated financial institution to enroll; and displaying the recipient's name, as registered with the recipient's bank account, to senders and asking senders to verify the recipient's contact information in the app before sending the payment.[17] In addition, EWS uses innovative data-driven technology to identify potential bad actors and intercept fraudulent transactions.[18]

B. Customer Education, Not This Enforcement Action, is Key to Protecting Consumers from Scams.

Not all scams can be stopped. Consumers have autonomy and, ultimately, a choice in how and when to spend their money, and they may fall prey to sophisticated scams.[19] This is why consumer education is a core component of protecting customers from those scams. To that end, participating institutions conspicuously advise their customers who use Zelle (and other P2P payment apps) to send money only to people and businesses they know and trust. With Zelle specifically, participating institutions include an in-app pop-up alert to ensure their customers know and have confirmed the payee and provide explicit statements to this effect to consumers during the payment process itself. EWS and the banking industry also participate in numerous initiatives to educate customers to help them identify, understand, and avoid common scams. Anti-phishing tutorials and educational campaigns—including *Amicus* American Bankers Association's

[17] *See, e.g.,* Zelle, *Security*, https://www.zelle.com/security (last visited Apr. 29, 2026).
[18] Zelle, *Zelle Fast Facts: History, Data Points and Common Questions*, *supra*.
[19] *See id.*

ongoing #BanksNeverAskThat campaign—advise customers not to click strange links, divulge passwords, or fall for impersonations of trusted individuals or businesses.[20]

Zelle is not completely immune from frauds and scams—no payment service can ever be. Bad actors are too widespread and persistent, and they are constantly changing their approaches to trick consumers and evade detection measures. In the small proportion of Zelle payments that are the product of unauthorized-transaction fraud or certain types of imposter scams, Network participants already make the affected user whole—in accordance with the Zelle Network Rules (the "Rules"), which go above and beyond what applicable law requires. The Rules require reimbursement for all instances of unauthorized payment—*and the NYAG does not deny that*. The Rules also provide reimbursement, beyond any legal requirement, for certain authorized payments made by bank customers who were tricked into making the payment under certain circumstances, for example, if the scammer poses as a government entity. (*See* Compl. ¶ 138).

The continuing fight against fraud and scams requires flexibility in how EWS and participating institutions engage. As technology evolves and advances, so do third-party wrongdoers' methods of separating consumers and small businesses from their money. For example, the start of the COVID-19 pandemic saw a surge in social media scams, with many scammers using "a social media message or friend request" to lure prospective victims into a long con.[21] The year 2024 saw a boom in so-called "task scams."[22] And now, scammers are using

[20] Am. Bankers Ass'n, *#BanksNeverAskThat*, https://www.banksneveraskthat.com/ (last visited Apr. 29, 2026).

[21] Fed. Trade Comm'n, *Scams Starting on Social Media Proliferate in Early 2020* (Oct. 21, 2020), https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2020/10/scams-starting-social-media-proliferate-early-2020 (last visited Apr. 29, 2026).

[22] Umar Shakir, *Game-Like "Task Scams" Stole More Than $220 Million in Six Months*, The Verge (Dec. 13, 2024), https://www.theverge.com/2024/12/13/24320391/ftc-task-scams-spotlight-warning (last visited Apr. 29, 2026).

generative artificial intelligence: a growing number of scammers are using deepfakes to impersonate loved ones or trusted authorities, often persuading victims to send money to address an emergency that does not exist.[23] EWS has responded to these emerging threats with consumer education and other measures, but the fight to protect consumers and small businesses requires constant vigilance and adaptation, as well as cooperation among various stakeholders, including financial institutions, law enforcement and those where the scams are taking place, *e.g.*, telecommunications and internet providers, and social media companies.[24]

As the NYAG admits, Zelle's track record demonstrates that EWS and participating institutions have kept pace with the evolving threats posed by fraudsters and scammers. However, the NYAG argues that a more-than-99.9% rate of incident-free payments is not good enough, and EWS must do more to "prevent or remedy fraud." (Compl. ¶ 155(b)). But by seeking so-called additional measures "necessary" to "protect consumers and limit consumer harm from fraudulent activity," *(id., Demand for Relief*), the NYAG seeks to strip EWS (and the institutions participating in Zelle) of the flexibility needed to respond to consumer threats in real time. In effect, the NYAG seeks to dictate how a critical nationwide payment service should be run. The NYAG's demands here would impose nebulous, ex-post constraints that risk becoming obsolete as soon as they are imposed and that would thrust both EWS and thousands of banks and other financial institutions across the country into a state of constant regulatory uncertainty as to what else the NYAG could next claim violates Section 63(12).

[23] *See* Zelle, *The Facts About Zelle and Scams, supra.*
[24] *Id.*

II. Holding EWS liable will deprive communities across New York and nationwide of access to a valuable financial service.

Federal law already imposes a duty of reimbursement for unauthorized transactions, and the NYAG nowhere claims these laws have been violated. *See* The Electronic Funds Transfer Act ("EFTA"), 15 U.S.C. §§ 1693a(12), 1693f(f); *New York by James v. Citibank, N.A.,* 763 F. Supp. 3d 496, 507 (S.D.N.Y. 2025) ("The EFTA allocates loss from unauthorized electronic fund transfers…from consumer accounts"); *see also Bank of Am. v. City & Cnty. of S.F.*, 309 F.3d 551, 564 (9th Cir. 2002) ("The EFTA was enacted to prevent fraud … in electronic fund transfers….").[25]

Rather, this lawsuit is about scams (induced fraud)—where an account holder authorizes a payment on Zelle, having been persuaded to do so "under false pretenses." (Compl. ¶¶ 44-45). But when a consumer is scammed into making payment on Zelle, the payment is often the *last step* in a course of dealings and communications on *other* platforms, about which EWS and the Zelle-participating institutions have no knowledge. In short, the NYAG's theory would effectively make Zelle *unique*, as the *only* payment method that makes financial institutions the insurers against scam transactions. The NYAG would do so without showing that participating institutions had the *ability* to control or prevent these transactions given the information outside their knowledge.

A. EWS cannot stop all scams and be forced to reimburse customers who authorize payments to bad actors.

The NYAG never explains how it expects EWS to stop (or else reimburse) all scams, especially given that neither EWS nor Zelle's participating institutions have any visibility into the facts and communications leading up to a payment procured by a scam. As the Complaint itself describes, scammers often use calls, texts, and social media to trick people into giving them their

[25] While the NYAG mentions "takeover fraud" (Compl. ¶ 44)—where a fraudster tricks a consumer into providing their account details and makes a payment himself—it does not (and cannot) allege that New Yorkers using Zelle were not made whole in instances of takeover fraud.

money under false pretenses. (*See* Compl. ¶ 111 (describing a "call … from an individual impersonating a Con Edison employee advising that the customer was delinquent on his energy bills"); *id.* ¶ 112 (describing a "text message purportedly from" a bank, followed by a phone call)). Consumers, not financial institutions, are best positioned to detect scams aimed at them and make decisions about how, when, and to whom to send money.

From years of experience, *Amici* know that EWS proactively identifies potential bad actors and removes bad actors from the Network when it becomes aware of them. But in circumstances where EWS does not know that a recipient is a bad actor, it cannot prevent a scam from occurring. (*See* Compl. ¶ 155(a)).

Technology alone will not solve the problem. As the Federal Reserve Bank of Kansas City observed, "[u]nlike an unauthorized payment initiated by a fraudster, which may be detected and stopped by a victim's financial institution, an authorized payment initiated by a victim (to a fraudster) will most likely be executed."[26] That is unsurprising: A scam payment often occurs only after a scammer "build[s] trust and carr[ies] out sustained manipulation" that is carried out "over days or weeks before any payment is made."[27] That degree of trust and manipulation is impossible for an institution to address using technological means alone—especially an institution whose only involvement is to receive a money-transfer instruction at the end of the scheme. For that reason, consumer awareness, education, and vigilance play the most critical role in preventing scams. By

[26] Ying Lei Toh, *Combating Authorized Push Payment Scams in Fast Payment Systems*, Fed. Rsrv. Bank of Kansas City (Nov. 15, 2024), https://www.kansascityfed.org/research/payments-system-research-briefings/combating-authorized-push-payment-scams-in-fast-payment-systems/ (last visited Apr. 29, 2026).

[27] The Payments Ass'n, *The New Origin of Authorised Push Payment (APP) Fraud: Evidence of Digital Platforms' Role and the Case for Shared Liability*, at 9, https://thepaymentsassociation.org/wp-content/uploads/2026/03/TPA_Whitepaper_AppFraud_Final.pdf (last visited Apr. 29, 2026).

the time the consumer is on an app making a payment, it is often impossible for either EWS or a bank to know that the consumer is being scammed.

B. Requiring EWS reimbursement for scams would ultimately harm consumers and smaller banks, while incentivizing scammers.

The NYAG's position that EWS should provide the "remedy" for all scams would place a disproportionate burden on financial institutions, especially thousands of small banks and credit unions, imposing liability for conduct they did not start and could not stop. (*See* Compl. ¶ 155(a)). The NYAG's apparent position—that EWS should be financially responsible for all scams for which Zelle is used—risks creating a moral hazard too: If users know that they have blanket scam protection, they may be less careful in their dealings.[28]

Liability here would have an especially negative impact on small financial institutions with fewer assets.[29] Ninety-five percent of the financial institutions in the Zelle network are community banks and credit unions, which together serve a broad variety of customers, including small businesses and residents of underserved communities.[30] Some community banks use Zelle to provide low-cost services to their customers in low-to-moderate income communities.[31]

Requiring reimbursement for every payment made by a Zelle customer in connection with a scam could drive many of these banks to consider withdrawing from the Zelle network entirely

---

[28] *See* Payment Sys. Regulator, *APP Fraud: Excess and Maximum Reimbursement Level for Faster Payments and CHAPS (CP23/6)*, at 8 (Aug. 2023), https://www.psr.org.uk/media/jplkxij4/cp23-6-app-fraud-excess-max-cap-consultation-paper-aug-2023.pdf (last visited Apr. 29, 2026).

[29] *See, e.g.,* Indep. Cmty. Bankers of Am., *Senate's Warren Continues Push for Bank Data on Zelle Fraud* (Oct. 2022), https://www.icba.org/w/senate-s-warren-continues-push-for-bank-data-on-zelle-fraud (last visited Apr. 29, 2026) ("Unlimited liability for P2P fraud under Reg E would have a disproportionate impact on community banks.").

[30] PYMNTS, *Velera Teams Up With Zelle to Drive Faster Payments for Smaller Credit Unions* (Apr. 14, 2025), https://www.pymnts.com/partnerships/2025/velera-teams-with-zelle-drive-faster-payments-smaller-credit-unions/ (last visited Apr. 29, 2026).

[31] *See id.*

or begin charging consumers a fee to use Zelle. That would deprive the communities served by these banks of critical access to a valuable financial tool, driving customers in those communities to *less secure* P2P payment apps that operate outside the federally regulated banking system. In turn, reduced participation in the Zelle network by small and community banks, which comprise such a substantial portion of the Zelle network, would inhibit Zelle's effectiveness for all users.

In summary, holding EWS responsible here would improperly shift liability to financial institutions for the conduct of bad actors, while also creating a moral hazard for consumers and failing to curb scam activity. It would impose disproportionate burdens on community institutions, jeopardizing access to a widely used P2P payment apps and driving users to less secure platforms. And it would improperly leverage a state law in an unprecedented manner to impose a nationwide standard that Congress considered and, in its judgment, *declined* to impose.[32] Compelling legal and policy considerations strongly militate against the expansion of Section 63(12) liability that the NYAG proposes here.

CONCLUSION

For the foregoing reasons, *Amici* respectfully urge the Court to grant EWS's motion to dismiss the NYAG's Complaint and award such further relief as the Court deems proper.

Dated: May 1, 2026
New York, New York

MANATT, PHELPS & PHILLIPS, LLP

By: _____

Brian S. Korn
Andrew L. Morrison
Samantha J. Katze
Eric M. Knight
Emily V. Whitely
7 Times Square

[32] *See* S. 4943, 118th Cong. (2024), https://www.congress.gov/bill/118th-congress/senate-bill/4943/all-info (last visited Apr. 29, 2026).

New York, New York 10036
Tel.: (212) 790-4500
Email: bkorn@manatt.com
Email: amorrison@manatt.com
Email: skatze@manatt.com
Email: eknight@manatt.com
Email: ewhitely@manatt.com

Richard E. Gottlieb (N.Y. Bar No. 2030203)
GLASER WEIL FINK HOWARD JORDAN & SHAPIRO, LLP
10250 Constellation Blvd., 19th Floor
Los Angeles, California 90067
Tel: (310) 556-7880
Email: rgottlieb@glaserweil.com

Attorneys for Amici Curiae American Bankers Association, Bank Policy Institute, Consumer Bankers Association, Independent Community Bankers Of America, National Bankers Association, and New York Bankers Association

CERTIFICATION OF WORD COUNT

In accordance Commercial Division Rule 23, I hereby certify that the annexed PROPOSED BRIEF OF *AMICI CURIAE* AMERICAN BANKERS ASSOCIATION, BANK POLICY INSTITUTE, CONSUMER BANKERS ASSOCIATION, INDEPENDENT COMMUNITY BANKERS OF AMERICA, NATIONAL BANKERS ASSOCIATION, AND NEW YORK BANKERS ASSOCIATION IN SUPPORT OF DEFENDANT'S MOTION TO DISMISS is 4,056 words in length, excluding the caption, table of contents, table of authorities, and signature block. This word count was prepared using the Word for Microsoft 365 application.

Dated: May 1, 2026
New York, New York

Brian S. Korn