

**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.

COMPLAINT

Index No. _____

Plaintiff People of the State of New York, by their attorney, Letitia James, Attorney General of the State of New York (the “OAG”), bring this action against Defendant Early Warning Services, LLC (“EWS” or “the Company”) alleging as follows:

INTRODUCTION

1. In the last decade, the rise of electronic payment apps, such as Venmo or Paypal, began to threaten banks’ traditional dominance over consumer payments. Before these new technologies rose to prominence, any consumer wanting to send money in a form other than cash generally was reliant on the methods provided by their banks, such as checks, in-person or telephonic transfers, and online bill payments. In recent years, however, consumers increasingly have looked beyond their banks to third-party providers to send funds electronically.

2. Defendant Early Warning Services, LLC, or EWS, an entity created by a group of the largest banks in the United States, was called upon to address this competitive threat. EWS developed Zelle, a service that provided banks’ customers with access to a new, instant-payment network, referred to herein as the Zelle network. EWS hurried Zelle to market in an effort to fend off increasing competition from Venmo, Paypal, and newer entrants like Cash App.

3. To quickly compete, EWS designed Zelle to be as simple, easy, and frictionless as possible. To access the Zelle network, all a consumer needs is an email address or mobile number, and a bank account or debit card. EWS imposes no upfront fees. Any consumer can sign up more than once, link multiple email addresses or mobile numbers to one or more accounts, and seamlessly transfer between existing and new accounts. Indeed, for many consumers with accounts at major banks, Zelle was automatically integrated into their banks' online and mobile banking platforms. And EWS lured in consumers by repeatedly highlighting the Company's connection to consumers' banks, assuring consumers that they could "safely send and receive money straight from your banking app" and that Zelle was "backed by the banks, so you know it's secure."

4. EWS's rush to market, however, came with a significant and foreseeable cost: EWS's key design decisions made the Zelle network an obvious conduit for fraudulent activity. A quick registration process and lack of verification made infiltration easy. The limited information displayed to consumers who send money over the Zelle network enabled fraudsters to use false or fraudulent email addresses to trick consumers. The Zelle network's emphasis on immediate funds availability facilitated quick getaways and deprived consumers of any chance to recover stolen funds. And the ability to seamlessly shift email addresses, bank accounts, and banks enabled fraudsters to engage in multiple ongoing frauds while evading detection or restriction.

5. As a result, from its launch the Zelle network has been teeming with fraudsters who have stolen staggering sums from consumers. By early 2019, [REDACTED] [REDACTED] its limited protocols and rules to prevent fraud were ineffective and that the Zelle network had been infiltrated by fraudsters, exposing millions of consumers to substantial harm. The Company's team responsible for

antifraud efforts, meanwhile, [REDACTED]

[REDACTED]

6. In July 2019, EWS finally developed and proposed a suite of modest, yet critical, security enhancements and changes to the rules governing the Zelle network that, working in combination, would reduce fraud over the Zelle network. These basic network safeguards, as they are referred to herein, were designed with specific goals in mind: to keep fraudsters off of the Zelle network and to ensure that identified fraudsters would be swiftly and permanently removed. However, [REDACTED] EWS abandoned the basic network safeguards in favor of [REDACTED]

[REDACTED] and that was otherwise wholly inadequate to prevent harm to consumers.

7. To make matters worse, for the next four years EWS failed to meaningfully enforce even the limited, and inadequate, network rules that did exist to detect, prevent, and address fraud. EWS knew that banks had violated its own network rules [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

8. EWS's decision to abandon the basic network safeguards in favor of [REDACTED] [REDACTED] and its lax enforcement of network rules caused catastrophic harm to millions of consumers. Over the next four years, consumers constantly fell victim to fraudsters operating over the Zelle network, losing hundreds of millions of dollars to preventable fraud, all while EWS and its banks earned hundreds of millions of dollars from Zelle's continued growth.

9. In 2023—and only after over a billion dollars in consumer losses from reported fraud and significant investigation and oversight from the federal Consumer Financial Protection

Bureau, or CFPB, and several members of Congress—EWS finally adopted each element of the basic network safeguards that it had originally proposed in 2019. The result was both immediate and immense: Despite overall transfers over the Zelle network growing by billions of dollars that year, consumer losses to reported fraudulent activity dropped by hundreds of millions of dollars. Yet these measures were too little too late: EWS did nothing to remedy the vast losses that consumers already suffered due to its failure to adopt the basic network safeguards in July 2019, and even with those safeguards in place Zelle continues to facilitate substantial fraudulent activity.

10. The OAG brings this action to enforce New York Executive Law § 63(12) and hold EWS accountable for the substantial harm to New Yorkers caused by the Company's creation of a payment network that was highly susceptible to fraudulent activity, that lacked the basic network safeguards, and that exposed millions of consumers to widespread fraud. Specifically, OAG seeks an order (i) enjoining EWS from engaging in the fraudulent practices described herein, (ii) ordering EWS to maintain the basic network safeguards and any other antifraud measures that are necessary to protect consumers and limit consumer harm from fraudulent activity; (iii) ordering EWS to provide an accounting of all New York consumers who reported losses to EWS or its participating banks; and (iv) awarding restitution, disgorgement, and other relief as appropriate.

PARTIES & JURISDICTION

11. Plaintiff is the People of the State of New York, by their attorney, Letitia James, the New York Attorney General and is authorized to take action to enjoin repeated and persistent fraudulent conduct under New York's Executive Law § 63(12).

12. Defendant Early Warning Services, LLC is a limited liability company that is authorized to do business in New York and is headquartered in Scottsdale, Arizona.

13. This Court has personal jurisdiction over Defendant because the cause of action arises from Defendant's supplying services in New York and from Defendant committing tortious acts within and without New York causing injury within New York. CPLR § 302.

14. Venue is proper because OAG resides in this county, because a substantial amount of the transactions, practices, and courses of conduct at issue occurred within this county, and because Defendant conducts business in this county. CPLR § 503.

FACTUAL ALLEGATIONS

I. EWS HASTILY LAUNCHED ZELLE AS A PAYMENT PLATFORM AND RAPIDLY GREW ITS TRANSACTION VOLUME AND CUSTOMER BASE

15. The Zelle network is an electronic payment platform owned and operated by EWS. EWS, in turn, is owned by seven banks: Bank of America, N.A. ("Bank of America"), Capital One, N.A. ("Capital One"), JPMorgan Chase Bank, N.A. ("JPMC"), PNC Bank, N.A., Truist Bank, Wells Fargo Bank, N.A. ("Wells Fargo"), and U.S. Bank, N.A. (collectively, the "Owner Banks"). The three largest Owner Banks are JPMC, Bank of America, and Wells Fargo.

16. EWS is governed by a Management Committee—lately renamed the EWS Board—comprised of representatives of each of the Owner Banks and EWS. The Management Committee makes decisions about the Zelle network, including setting rules that govern how banks, credit unions, and other financial institutions, referred to herein as participating banks, can use Zelle.

17. Zelle's inception traces back to EWS's acquisition of clearXchange, a digital payments network, from four of the Owner Banks—Bank of America, JPMC, Wells Fargo, and Capital One—in January 2016. Upon completing the acquisition, EWS announced its intention to leverage clearXchange's technology to "eliminat[e] friction from real-time payments" and create "the largest, most secure real-time payments ecosystem in the U.S." EWS added: "we believe the best payments solution is one developed, secured, and delivered by financial institutions."

18. At the time, nonbank electronic payment apps, such as Paypal and Venmo, were flourishing. For instance, Venmo reported that more than \$1 billion of payments were made in January 2016—a 250% increase from January 2015, and an over 1,000% increase from January 2014. As these electronic platforms captured an increasing share of electronic fund transfers by promising free, instant transfers between users, banks risked losing their traditional dominance over payments that rely upon access to consumer bank accounts, which had long enabled banks to harvest enormous amounts of fees and financial data from their customers.

19. Eager to establish a foothold in the burgeoning electronic payment market, EWS and the participating banks [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

20. Upon launching in 2017, EWS rapidly made Zelle available to as many consumers as possible. To accomplish this, EWS designed Zelle to be free and made it frictionless to enroll, as alleged in detail below. EWS further turbo-charged enrollment by embedding Zelle directly within mobile banking apps and websites for participating banks. At Zelle’s launch, EWS announced that the Zelle network would be “conveniently available” in the mobile-banking apps of “more than 86-million U.S. mobile banking consumers” with “no additional app to download.” The goal, EWS publicly stated at Zelle’s launch, was “removing friction from finance.”

21. [REDACTED]

[REDACTED]

As a result of this feature, EWS directly—and

irremovably—offered Zelle access to tens of millions of consumers, including millions of New Yorkers, almost immediately upon launch. And EWS’s direct integration of Zelle into mobile-banking apps also enabled it to immediately and directly reach many more consumers each time a new bank contracted with EWS to become a participating bank in the Zelle network.

22. By July 2018, when EWS announced Zelle’s “first anniversary,” the Zelle network had already processed \$94 billion in payments over 320 million transfers. EWS also reported that more than 100 million consumers had direct access to Zelle. Later that year, EWS’s CEO declared Zelle “one of the fastest growing consumer financial brands in history.”

23. Zelle continued to grow rapidly in 2019, when it processed 743 million transfers valued at \$187 billion. By the end of 2019, EWS boasted that nearly 400 participating banks were linked to the Zelle network, “representing nearly 70% of all U.S. checking accounts.”

II. EWS ADVERTISED ZELLE AS A SAFE AND SECURE WAY FOR CONSUMERS TO MAKE ELECTRONIC PAYMENTS

24. From its launch, EWS has assured consumers through a variety of channels that Zelle was “safe” or “secure” and that banks’ participation in the Zelle network means consumers will be protected from fraud. The June 2017 press release announcing Zelle, for example, promised that Zelle “will make digital payments a fast, safe and easy alternative to checks and cash.”

25. EWS issued another press release three months later, assuring consumers that they can use Zelle to “send and receive money fast – all with the peace-of-mind that your transactions will be backed by the security of your trusted financial institution.”

26. Over the next few months, EWS launched a multi-media advertising “blitz” to encourage consumers to use Zelle and [REDACTED]

27. EWS’s campaign included ads in the New York City subway, full page ads in People and Travel + Leisure magazines sold in New York, billboards appearing in Penn Station,

Times Square, and Barclays Center, and television ads airing in New York during the NFL playoffs, the Grammys, the NBA All-Star Game and the Super Bowl pregame show.

28. In one of those ads, which began airing on television soon after Zelle's launch and still appears on the social media page of one of EWS's paid marketing partners as of the filing of this Complaint, EWS suggested that consumers can use Zelle "to send money safely," and that Zelle was "backed by the banks, so you know it's secure."

29. EWS also aggressively marketed that Zelle is built directly into mobile banking apps, exploiting consumers' perception that this linkage guaranteed Zelle's safety. Ads in the New York City subway, on New York City billboards, and on full pages of People and Travel + Leisure magazine advised consumers to look for Zelle "in your mobile banking app." [REDACTED]

[REDACTED]

30. In September 2019, a Zelle executive publicly attributed the "popularity and success of *Zelle*" to "trust in using a service included in mobile banking apps."

31. EWS continued to provide similar assurances for years. In late 2020, EWS [REDACTED]
[REDACTED]
[REDACTED] In March 2022, EWS [REDACTED]

[REDACTED] And from at least early 2022 through the filing of this Complaint, EWS has assured consumers on the Zelle website that they can "use Zelle® to safely send and receive money straight from your banking app."

III. EWS'S FRICTIONLESS DESIGN OF THE ZELLE NETWORK MADE IT AN ATTRACTIVE VEHICLE FOR FRAUDSTERS

32. EWS's rush to get Zelle to market in an effort to compete resulted in a payment network that, contrary to its representations, was rife with fraudulent activity.

A. EWS's Design of the Zelle Network Prioritized Speed and Easy Access

33. EWS designed the Zelle network to be effectively frictionless. There are no fees to enroll in Zelle, and registration is designed to be quick and simple. Any person with a bank account at one of the more than 2,200 participating banks can register. And from 2017 until very recently, a consumer without a bank account at a participating bank could register with the Zelle network by linking a debit card to the mobile application operated by EWS (the "Zelle App").

34. A user enrolls in Zelle by providing an email address or mobile number, which EWS refers to as a "token" over the Zelle network. A user often must validate a token using a one-time passcode that is delivered to the provided email address or mobile number.

35. A user can register multiple tokens to a single bank account using different email addresses or mobile numbers. A user also can register additional tokens with different bank accounts at other participating banks using different email addresses or mobile numbers. And a user can re-assign a token from one bank account to another bank account.

36. [REDACTED]

[REDACTED]

37. Once a user with an account at a participating bank enrolls in Zelle, the user can access the Zelle network through the banks' online website and mobile application. Many banks embed Zelle in these platforms without any option for users to remove them.

38. Until recently, a user who enrolled in Zelle through the Zelle App using a debit card linked to the Zelle network could access the Zelle network through the Zelle App.

39. Once enrolled, a user sends money over the Zelle network by entering the token of a recipient in the form of an email address or mobile number, plus the amount to be sent. If the token is registered with the Zelle network, the user's requested funds are deposited in nearly real-time into the bank account associated with the entered token. If the token is unregistered, meaning that it has not been enrolled in Zelle, the user's requested funds still may be sent. In that case, EWS will send a message regarding the pending transfer to the email address or mobile number informing its owner that the funds can be accessed by enrolling with Zelle using that email address or mobile number and linking a bank account or debit card to the Zelle network.

40. EWS maintains a Zelle Network Directory that matches registered tokens with the linked user, the participating bank, and the user's bank account information. [REDACTED]

[REDACTED]

41. When a Zelle user enters a request to transfer funds over the Zelle network, EWS will match the token provided by the user to its profile in the Zelle Network Directory and send a message to the recipient's participating bank about the transfer. EWS and the participating banks agree that the recipient's participating bank will then make the funds available in the recipient's account, treating completed transfers as irrevocable. Participating banks then handle settlement of all transfers completed over the Zelle network among themselves at the end of the day.

42. Finally, the Zelle network is governed by a series of rules, referred to herein as the network rules, adopted by EWS's Management Committee. EWS is responsible for enforcing the network rules against participating banks and is empowered to assess fees for noncompliance. These network rules address, among other things, requirements for participating banks to report, respond to, and reimburse their customers for fraud-based losses over the Zelle network.

B. EWS's Design Decisions Enhanced Fraudsters' Ability to Effectively Swindle Consumers over the Zelle Network While Evading Detection

43. EWS's frictionless design of the Zelle network made it an attractive vehicle for fraudsters to steal money from Zelle users through a variety of fraudulent schemes.

44. One common form of fraud over the Zelle network is takeover fraud, which EWS refers to internally as simply "fraud." Takeover fraud occurs when a fraudster obtains improper access to a Zelle user's account or device and uses such access to execute a transfer that the Zelle user did not authorize or benefit from. Examples include fraudsters who take over a Zelle user's mobile device through hacks or SIM swaps and fraudsters who trick unsuspecting users into providing credentials or other security information to obtain access to users' accounts.

45. Another common form of fraud over the Zelle network is induced fraud, which EWS refers to internally as "scams," and which, at Zelle's launch, the Company did not even track. Induced fraud occurs when a fraudster convinces a Zelle user to send funds under false pretenses, such as for non-existent goods or services, in pursuit of false romantic promises, or under the guise of instructions by a trusted institution, such as a user's bank or a governmental entity.

46. EWS's design of a quick and frictionless enrollment process for the Zelle network made the Zelle network a compelling vector for both takeover fraud and induced fraud:

a. Initial sign-up is designed to be fast, simple, and easy. Potential users, including fraudsters, generally can register with Zelle using nothing more than a bank account and either an email address or U.S. mobile number. Verification requires a potential user merely to demonstrate that they have access to the email address or mobile number that they provide and that will be the token over the Zelle network, typically by entering a one-time passcode.

b. [REDACTED]

[REDACTED]

[REDACTED] for example, a

fraudster can obtain a one-time passcode from a Zelle user and use that code to reassign the user's token to a bank account the fraudster controls.

47. EWS's decisions about the Zelle network's transfer mechanics and user experience also facilitate both of the common forms of fraud over the Zelle network:

a. Fraudsters need to provide Zelle users with only an email address or mobile number to facilitate Zelle network transfers. As a result, a Zelle user at risk to an ongoing fraud has no ready means of ascertaining the true identity of the holder of the token to which funds are being sent. In addition, at launch and for several years after, a fraudster could register misleading email addresses as tokens, including addresses that appear to be associated with trusted actors such as the user's participating bank, a governmental entity, or even Zelle itself.

b. EWS does not require participating banks to display any information about a recipient, other than first name, to a Zelle user when transferring funds. As a result, a Zelle user at risk to an ongoing fraud often lacks access to additional information that might enable them to avoid future losses, such as the recipient's last name or how long the recipient has been using Zelle.

c. EWS permits transfers to unregistered tokens, meaning email addresses or mobile numbers that have not been enrolled in Zelle. As a result, when a Zelle user at risk to an ongoing fraud transfers funds to a fraudster's unregistered

token, that user will not be provided a first name or any additional information other than the fraudster's handpicked email address or mobile number.

d. [REDACTED]
[REDACTED]
[REDACTED].

48. EWS's emphasis on immediate funds availability likewise makes Zelle attractive to fraudsters: Because fraudulently obtained funds typically are made available to recipients immediately, by the time a Zelle user realizes that they have been targeted by an ongoing fraud, the funds sent over the Zelle network are already withdrawn and lost to fraudsters.

49. Finally, EWS's frictionless design of the Zelle network enables fraudsters to engage in multiple schemes at once while readily evading detection or restriction:

a. EWS today permits one user to register up to five tokens linked to a single bank account, and in earlier periods permitted registration of more than five tokens. As a result, a fraudster can engage in multiple ongoing frauds targeting multiple consumers using different tokens linked to the same bank account. And even if a Zelle user reports takeover or induced fraud associated with one token, the fraudster can continue to use other tokens to facilitate more ongoing fraud.

b. EWS permits a user to switch the registration of a token between different participating banks, including for years the ability to re-register several tokens in short periods. As a result, a fraudster can move tokens among bank accounts at different participating banks, limiting the risk that a single participating bank will identify a particular token as linked to continuing fraud.

c. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

50. Notwithstanding the above flaws, EWS and participating banks have had, since the launch of Zelle, some tools available to limit consumer harm from common frauds.

51. For example, EWS, along with participating banks, has the technical capability to restrict a token, meaning that any attempt to send funds to the email address or mobile number associated with the restricted token will not be completed over the Zelle network.

52. The participating banks also have the capability to pause or block any transfers over the Zelle network that they consider suspicious or risky based on parameters that they determine.

EWS, however, does not [REDACTED]

[REDACTED] EWS also has not [REDACTED]

[REDACTED]

[REDACTED]

IV. FOLLOWING LAUNCH, [REDACTED]
[REDACTED] THE ZELLE NETWORK HAD BECOME RIFE WITH
FRAUD AND THAT EWS HAD DONE LITTLE TO ADDRESS THE PROBLEM

53. Upon Zelle's 2017 launch, fraud quickly proliferated over the Zelle network.

54. In the first year, one large participating bank [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

55. Another large participating bank [REDACTED]

[REDACTED]

[REDACTED] That bank's [REDACTED]

[REDACTED]

56. A third large participating bank [REDACTED]

[REDACTED]

57. And EWS itself [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

58. During this early period, [REDACTED]

[REDACTED]

59. The next year, as Zelle continued to grow rapidly, the prevalence of fraud over the Zelle network did as well. One participating bank [REDACTED]

[REDACTED] Another participating bank

[REDACTED]

[REDACTED]

60. By 2019, EWS [REDACTED]

[REDACTED]

[REDACTED]

61. For example, EWS [REDACTED]

[REDACTED] At the time, however,

EWS permitted a Zelle user to associate up to 20 unique tokens with a participating bank.

62. [REDACTED]

[REDACTED]

[REDACTED]

63. EWS and participating banks also regularly received complaints from Zelle users who had been subject to fraud involving email addresses that appeared to be associated with banks, government entities, and even “Zelle” itself. At the time, however, EWS imposed no restrictions to limit a fraudster’s ability to register with a suspicious email address.

64. When participating banks received complaints from Zelle users about fraud, EWS did not ensure timely reporting and action. At launch, for example, EWS did not require participating banks to report induced fraud at all. And EWS [REDACTED]

[REDACTED]

65. Moreover, while EWS’s network rules require prompt reporting of takeover fraud and (eventually) induced fraud to enable EWS or participating banks to impose restrictions on fraudsters, in practice EWS has allowed participating banks to make such reports [REDACTED] after the events occurred and banks were notified by consumers, allowing known or suspected fraudsters to continue to use access to the Zelle network to victimize additional consumers.

66. By early 2019, EWS [REDACTED]

[REDACTED]

[REDACTED] As a result, [REDACTED]

[REDACTED]

[REDACTED] A few months later, [REDACTED]

[REDACTED]

67. [REDACTED]

68. Tellingly, one participating bank [REDACTED]

[REDACTED] That

bank [REDACTED]

[REDACTED] EWS [REDACTED]

69. [REDACTED]

[REDACTED] In 2017,

[REDACTED] In 2018, [REDACTED]

[REDACTED] And in 2019, [REDACTED]

**V. EWS DEVELOPED AND PROPOSED THE BASIC NETWORK SAFEGUARDS
IN JULY 2019 BUT DECLINED TO ADOPT THEM AND INSTEAD [REDACTED]
[REDACTED] AND WEAK ENFORCEMENT**

70. By no later than July 2019, EWS recognized that it needed to take significant measures to combat fraudulent activity. That month, EWS identified the basic network safeguards

to accomplish this goal but then failed to adopt them. Instead, the Company adopted [REDACTED] [REDACTED] that, coupled with EWS's continued lax enforcement of the network rules regarding fraud reporting, allowed fraudsters to continue to run rampant.

A. EWS Developed and Proposed the Basic Network Safeguards in July 2019 that Would Have Substantially Limited the Prevalence Fraud

71. In July 2019, EWS developed and proposed to certain participating banks the basic network safeguards, [REDACTED]

[REDACTED] When implemented as a package, the basic network safeguards were intended to prevent fraudsters from accessing the Zelle network and to promptly and permanently remove those that did. These safeguards [REDACTED]

[REDACTED] as described below.

72. [REDACTED]. In July 2019, EWS [REDACTED]

[REDACTED] For induced fraud, for example, before the token belonging to the fraudster could be restricted, [REDACTED]

[REDACTED] During this process, [REDACTED]

[REDACTED] the fraudster could continue to use that token for other fraudulent activity. And even if the token ultimately was restricted, the fraudster could turn to other registered tokens.

73. As one of the basic network safeguards, EWS [REDACTED]

[REDACTED]

[REDACTED] EWS [REDACTED]

[REDACTED]

74. However, the efficacy of [REDACTED] still depended on fixing other glaring flaws in Zelle network's antifraud policies and procedures. For example, delays by participating banks in reporting potential or confirmed fraud to EWS would likewise delay EWS in restricting the fraudster's tokens, enabling fraudsters to continue to operate.

75. Moreover, [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

76. [REDACTED] In July 2019, the Zelle network rules permitted sending banks to [REDACTED]

[REDACTED]

77. As part of the basic network safeguards, EWS [REDACTED]

[REDACTED]

[REDACTED]

78. [REDACTED]

[REDACTED]

[REDACTED] However, [REDACTED]

[REDACTED]

[REDACTED]

79. [REDACTED] In July 2019, neither EWS nor the receiving banks [REDACTED]

[REDACTED]

[REDACTED] Indeed, at Zelle's launch, EWS did not even mandate that participating banks report induced fraud to the Company.

80. As the final piece of the basic network safeguards, EWS [REDACTED]

[REDACTED]

[REDACTED] At the time, EWS

[REDACTED]

[REDACTED] EWS [REDACTED]

[REDACTED]

[REDACTED]

81. On or about July 2019, EWS [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] EWS [REDACTED]

[REDACTED]

[REDACTED]

B. EWS [REDACTED]
[REDACTED]

82. [REDACTED]

[REDACTED] EWS did not adopt them in 2019 or for nearly four years thereafter. Instead, EWS

[REDACTED]

83. In particular, [REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED] the EWS team did not adopt the proposed basic network safeguards for years. [REDACTED]

84. [REDACTED] EWS developed and implemented the following [REDACTED]:

a. *First*, EWS [REDACTED]

[REDACTED]
[REDACTED] Unlike the proposed basic network safeguards, [REDACTED]
[REDACTED]
[REDACTED]

b. *Second*, participating banks [REDACTED]

[REDACTED]

c. *Third*, [REDACTED]

[REDACTED]
[REDACTED]

85. The alternative [REDACTED] had obvious flaws that made it destined to fail at effectively limiting fraudulent activity over the Zelle network:

86. For one, because EWS [REDACTED]

[REDACTED]

[REDACTED]

87. Moreover, fraudsters' ability to register multiple tokens and move them from bank to bank [REDACTED]

88. [REDACTED]

[REDACTED]

[REDACTED] In other words, banks [REDACTED]

[REDACTED] Indeed, one of the largest participating banks' customers [REDACTED]

[REDACTED]

89. Finally, [REDACTED]

[REDACTED]

[REDACTED]

C. EWS Failed to Meaningfully Enforce the Existing Network Rules

90. In isolation, EWS's failure to adopt the basic network safeguards in 2019 and for years thereafter [REDACTED] was bad enough. But that decision was made all the worse by EWS all but abandoning its role in enforcing the network rules.

91. In particular, the network rules provided for the imposition of "non-compliance fees" on participating banks when EWS determines that they have violated those rules.

92. For years, EWS knew that participating banks were systematically violating network rules that, though inadequate, were designed to detect, prevent, and address fraud. Yet the Company failed to meaningfully enforce these rules against delinquent participating banks.

93. For example, the network rules have long required (i) sending banks to report fraudulent activity and (ii) receiving banks to review and respond to reported fraud [REDACTED]

[REDACTED] EWS knew that participating banks routinely violated those requirements.

94. As early as 2019, EWS [REDACTED]

[REDACTED] EWS also [REDACTED]

95. Indeed, [REDACTED]

96. Despite being aware of widespread violations of reporting and other network rule requirements, EWS [REDACTED] EWS

97. Even in the few cases where EWS [REDACTED]

98. EWS's [REDACTED]

99. In September 2019, however, EWS [REDACTED]

100. [REDACTED]

[REDACTED] JPMC's parent company, for instance, generated an average of \$10 billion in net revenues per month in 2020. [REDACTED]

101. [REDACTED]

[REDACTED] Between 2020 and 2022, [REDACTED]

[REDACTED] During that three-year period, [REDACTED]

102. Moreover, even when EWS [REDACTED]

[REDACTED] In 2021, [REDACTED]

[REDACTED] In 2019—

[REDACTED]—EWS [REDACTED]

VI. FOR THE NEXT FOUR YEARS, CONSUMERS IN NEW YORK AND ELSEWHERE LOST HUNDREDS OF MILLIONS OF DOLLARS TO FRAUD WHILE EWS CONTINUED TO RAPIDLY GROW THE ZELLE NETWORK

103. EWS' refusal to adopt the basic network safeguards or enforce its existing rules had a predictable effect: New York consumers lost millions to fraudulent activity.

A. EWS Tracked Fraudulent Activity over the Zelle Network and Knew that it Caused Hundreds of Millions of Dollars in Consumer Harm

104. EWS closely tracked fraudulent activity reported over the Zelle network. EWS

[REDACTED]

[REDACTED] EWS knew that fraudulent activity continued to cost consumers ever-increasing amounts totaling hundreds of millions of dollars each year.

105. EWS [REDACTED]

[REDACTED]

106. In 2021, [REDACTED]

[REDACTED]

[REDACTED]

107. With respect to induced fraud specifically, EWS [REDACTED]

[REDACTED]

[REDACTED]

108. Fraudulent activity perpetrated over the Zelle network continued to balloon though 2022. That year, EWS [REDACTED]

[REDACTED] EWS [REDACTED]

[REDACTED]

109. All told, from 2019 through 2022, [REDACTED]

[REDACTED]. EWS

[REDACTED]

110. One New York consumer signed a contract to purchase a puppy in November 2020 and was told by the purported seller that “you have to make the payment using chase quickpay with Zelle.” The consumer believed using Zelle was safe since it was recommended by his bank.

After the consumer transferred \$1,100 via Zelle to an account name that matched the purported seller in the contract, the purported seller requested another \$1,500 for shipment insurance, which the consumer also paid through Zelle. When the purported seller demanded still more money before delivering the puppy, the consumer realized he had been defrauded, but after reporting the induced fraud to JPMC, he was advised that neither “Chase nor Zelle could assist.”

111. Another New York consumer received a call in August 2021 from an individual impersonating a Con Edison employee advising that the consumer was delinquent on his energy bills and that his “electricity was going to be shut off that day” unless he paid Con Edison via Zelle. During the call, the fraudster repeatedly assured the consumer that they worked for Con Edison, provided a title at the company, and identified “Coned Billing” as the name associated with the account. The consumer transferred \$1,476.89 to a Zelle account named “Coned Billing” and was later told by JPMC that “they can’t get me that money back.”

112. In November 2021, a New York consumer received a text message purportedly from JPMC asking for confirmation of a \$1,090.54 transaction. When the customer replied that he had not authorized the transaction, he received a phone call from a purported JPMC representative seeking confirmation. The fraudster stated “the exact dollar amount in my account” which “convinced” the customer he was “speaking with Chase.” The fraudster asked if the consumer had authorized a \$2,000 Zelle transfer to a different bank, and when the consumer said he had not, the fraudster directed the consumer to send himself \$2,000 over the Zelle network to “cancel out this payment.” When the consumer did so, the funds went to an unknown account and the fraudster hung up. The consumer contacted JPMC and EWS, but his claim was repeatedly denied.

113. A longtime New York Citibank consumer received a text message from Citibank on April 3, 2023 asking whether he had initiated a Zelle transfer, to which he responded: “no.”

The same day, a \$2,500 Zelle transfer was executed on his account to a name that the consumer did not recognize, two new Citibank checking accounts were fraudulently opened, and a \$2,499 Zelle transfer from a new account was executed. The consumer had never made a Zelle transfer before. The consumer then had automatic withdrawals from his Citibank account fail and incurred fees as a result. When the consumer contacted Citibank about the fraudulent activity, Citibank ultimately reversed and credited the \$2,499 Zelle transfer from the fraudulent account, but denied his claim related to the fraudulent \$2,500 Zelle transfer from his real account.

114. EWS was aware of these and millions more instances of fraudulent activity perpetrated over the Zelle network. In fact, the Company [REDACTED]

[REDACTED]

[REDACTED]

115. In May 2021, EWS [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

116. In September 2021, [REDACTED]

[REDACTED]

[REDACTED]

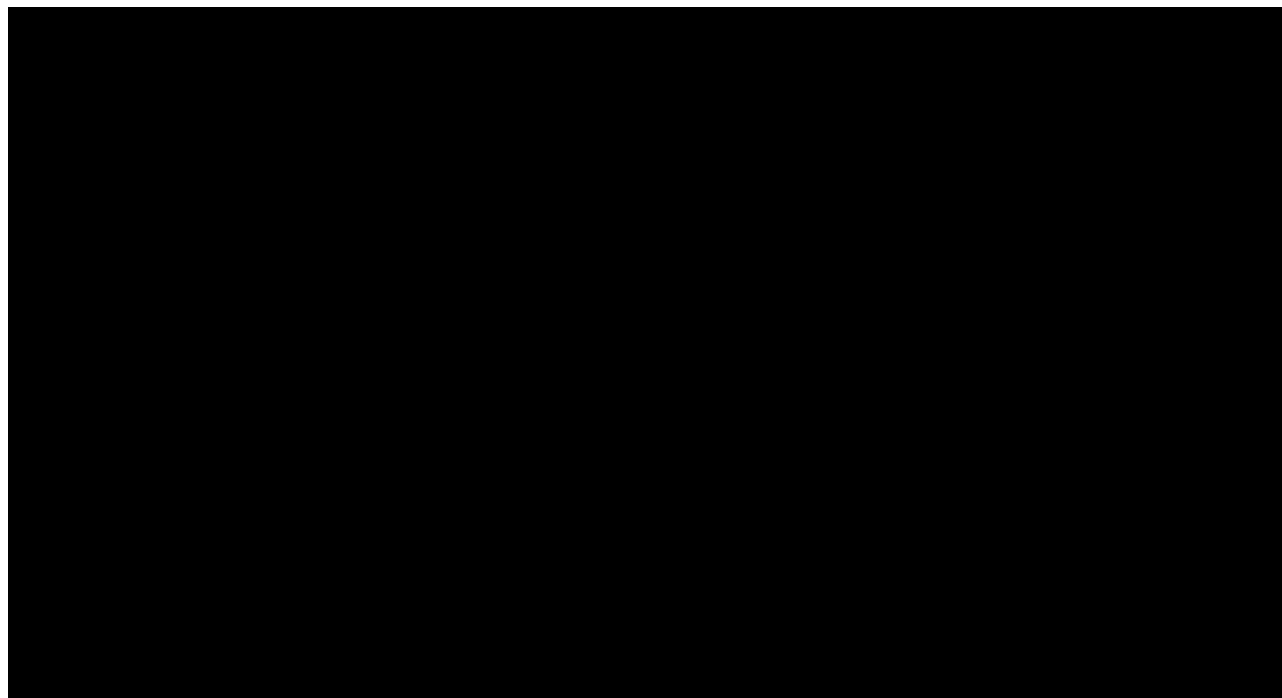
[REDACTED]

117. [REDACTED]

[REDACTED] As shown below, EWS [REDACTED]

[REDACTED]

[REDACTED]. EWS [REDACTED]



118. Similarly, in November 2021, EWS [REDACTED]

[REDACTED]
[REDACTED]

119. In 2022, EWS [REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]

120. For years, however, EWS continued to provide free reign for fraudsters to exploit consumer after consumer [REDACTED] and refused to hold participating banks accountable for harm to consumers from fraudulent activity.

B. EWS Continued to Rapidly Grow the Zelle Network Without Implementing the Network Safeguards or Other Effective Measures

121. While EWS's decision to disregard effective security measures caused substantial losses to consumers, they imposed few costs on the Company. To the contrary, EWS's business model enabled it to reap the benefits of Zelle's growth [REDACTED]

122. Participating banks [REDACTED]

[REDACTED] Participating banks [REDACTED]

[REDACTED] Participating banks [REDACTED]

[REDACTED] For some of the largest participating banks, [REDACTED]

123. [REDACTED]

124. In addition, EWS's meager antifraud measures, as well as its lax enforcement practices, made it cheaper for banks to participate in the Zelle network and easier for EWS to sign up and retain banks. This, too, benefited EWS by enabling it to more quickly expand the Zelle network and capture market share from other electronic payment platforms.

125. EWS's prioritization of the rapid growth of Zelle at the expense of consumers had its intended effect: Zelle quickly climbed to the top of the electronic payment market.

126. From 2019 to 2022, Zelle expanded the total dollar amount of payments processed annually by 236%, the total number of transfers processed annually by 210%, and the total number

of participating banks by 135%. The Company's revenues from Zelle [REDACTED] during this period, [REDACTED] to over \$200 million in 2022.

127. In 2022, EWS processed 2.3 billion payments with a total value of \$629 billion over the Zelle network. This included, upon information and belief, tens of billions of dollars in transfers by New York consumers. By the end of 2022, EWS had also contracted with over 1,800 participating banks, including several banks chartered and headquartered in New York.

128. Earlier that year, EWS highlighted that Zelle had "rapidly grown to become the largest U.S. P2P payments network by total payments value sent, with payment flows that are now twice the size of the next largest standalone competitor." EWS touted the Zelle network's success as a "testament that if financial institutions build it, they will come."

VII. FACING MOUNTING PRESSURE FROM CONGRESS AND REGULATORS, EWS EVENTUALLY ADOPTED THE BASIC NETWORK SAFEGUARDS

129. Notwithstanding EWS's public proclamations of Zelle's success, EWS [REDACTED]

[REDACTED]

[REDACTED] As early as June 2021, [REDACTED]

[REDACTED]

130. [REDACTED] the CFPB had launched an investigation into fraudulent activity over the Zelle network [REDACTED]

[REDACTED]

131. In April 2022, Senator Elizabeth Warren opened an investigation into the Zelle network, citing "disturbing reports of a rise in fraud and scams" and "the ongoing failure by Zelle or the banks that own this service to address this fraud and provide appropriate redress."

132. Senators Warren, Robert Menendez, and Jack Reed wrote to EWS on April 25, 2022 seeking information about the frequency of fraudulent activity over the Zelle network and its

policies for redressing consumers. Senator Warren and six other Senators also sent letters to each of the Owner Banks in July 2022 seeking similar information.

133. Over the ensuing months, EWS produced information in response to the Senate requests, as did some of the Owner Banks. In October 2022, Senator Warren publicly released a report summarizing the findings of her office's investigation. The report concluded, based on the information provided by the EWS and several Owner Banks, that "Zelle facilitates fraudulent activity of many kinds," and that "fraud and theft on Zelle are widespread and growing, with consumers losing millions each year." The report also urged regulators, including the CFPB, to "step in" to protect consumers and ensure a "fair and consistent process for everyone."

134. [REDACTED] the CFPB continued to press its investigation [REDACTED] [REDACTED]

[REDACTED] EWS [REDACTED]
[REDACTED]
[REDACTED]

135. Only in [REDACTED] 2023, as EWS began to face the music for facilitating large scale fraudulent activity, did the Company fully implement the basic network safeguards.

136. [REDACTED] In [REDACTED] 2022, EWS [REDACTED]
[REDACTED]

[REDACTED] In [REDACTED] 2022, EWS [REDACTED]
[REDACTED] And in [REDACTED] 2022, EWS [REDACTED]
[REDACTED]

[REDACTED] Together, these measures finally enabled EWS [REDACTED]
[REDACTED]

137. [REDACTED] Effective [REDACTED] 2023, EWS [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] This enabled EWS [REDACTED]

[REDACTED]

138. [REDACTED] Effective [REDACTED] 2023, EWS [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

139. EWS had identified each of these basic network safeguards in 2019 as a necessary and appropriate component of a suite of modest measures to limit harm to consumers from fraud. But by the time EWS implemented these changes, nearly four years later, New York users had lost tens of millions, if not hundreds of millions, of dollars to preventable fraudulent activity.

VIII. ADOPTION OF THE NETWORK SAFEGUARDS SIGNIFICANTLY DECREASED FRAUDULENT ACTIVITY OVER THE ZELLE NETWORK

140. In 2023, the first year in which the complete suite of basic network safeguards was implemented, consumer losses from fraudulent activity over the Zelle network decreased [REDACTED]

[REDACTED]

141. In total, EWS's [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

142. [REDACTED] total payments over the Zelle network increased by nearly \$200 billion in 2023 as Zelle continued to grow. Taking that increase in transfer volume into account, [REDACTED]

[REDACTED]

143. This drastic reduction in consumer harm was substantially caused by EWS's belated adoption of the full suite of basic network safeguards by the middle of 2023.

144. EWS's belated implementation of [REDACTED]

[REDACTED]

[REDACTED] As alleged above, EWS had recognized for years the dramatic downward impact that these measures would have on its fraud rates, and they in fact did have that effect once implemented.

145. EWS's belated implementation of [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] Again, as alleged above, EWS

[REDACTED]

[REDACTED]

146. EWS's multi-year failure to impose the basic network safeguards caused staggering harm to consumers. If the basic network safeguards had been implemented even one year earlier and EWS [REDACTED]

[REDACTED]

147. [REDACTED]

[REDACTED]

[REDACTED]

148. However, EWS did not do any re-assessment of consumer harm [REDACTED]

[REDACTED] that occurred from 2019 to 2023.

IX. THE CFPB FILED BUT THEN DROPPED A LAWSUIT SEEKING TO HOLD EWS ACCOUNTABLE FOR ZELLE NETWORK FRAUD

149. The CFPB's investigation culminated in a lawsuit filed on December 20, 2024 against EWS and three of the Owner Banks in Arizona federal court.

150. The CFPB's complaint alleged: "Shortly after Zelle's launch, significant problems, including fraud being perpetrated on consumers using Zelle, quickly became apparent. But Defendants did not take meaningful action to address these clear defects for years." It further alleged that "Zelle users lost hundreds of millions of dollars to fraud" due to EWS's failures to adopt "appropriate measures to prevent, detect, limit, and address Zelle fraud."

151. On January 31, 2025, President Trump fired the CFPB Director Rohit Chopra. President Trump designated Russell Vought as Acting Director of the CFPB a week later.

152. On March 4, 2025, before EWS or any other defendant answered the CFPB's complaint, the CFPB filed a one-page notice dismissing the case as against all defendants with prejudice. The notice did not provide any explanation for the dismissal.

CAUSES OF ACTION

**FIRST CAUSE OF ACTION
Executive Law § 63(12) (Fraud)**

153. Plaintiff repeats and realleges the allegations in paragraphs 1 to 152 above.

154. New York's Executive Law § 63(12) authorizes Plaintiff to seek injunctive and other equitable relief when any individual or entity engages in repeated and persistent fraud in the

carrying on, conducting, or transacting of business. Such fraudulent conduct includes that which has the capacity or tendency to create an atmosphere conducive to fraud.

155. EWS has engaged in fraud in connection with the Zelle network, its electronic payment platform offered to New York consumers, in at least the following respects:

a. having created an atmosphere conducive to fraud by establishing the Zelle network, creating the Zelle App, and unilaterally integrating the Zelle network directly into consumers' banking apps and websites, knowing that its design and features, and glaring flaws in its antifraud measures, render it highly susceptible to fraudulent activity, which was and is in fact widespread over the Zelle network, yet failing to meaningfully enforce its own network rules or take basic, known, effective measures to prevent or remedy fraud; and

b. promoting and marketing, as well as advising and assisting participating banks in promoting and marketing, the safety and security of the Zelle network and its participating banks when in fact Zelle was and is not safe or secure from fraudsters, EWS did not require reimbursement for induced fraud, and EWS failed to implement basic, known, effective measures to prevent or remedy fraud.

156. By reason of the conduct alleged herein, Defendant has engaged in and continues to engage in repeated and persistent fraud in violation of Executive Law § 63(12).

DEMAND FOR RELIEF

WHEREFORE, Plaintiff respectfully requests that the Court issued an order and judgment under Executive Law § 63(12):

a. permanently enjoining Defendant, its agents, trustees, employees, successors, heirs, and assigns; and any other person under their direction or control, whether acting individually or in concert with others, or through any corporate or other entity or device through which one or more of them

may now or hereafter act or conduct business, from engaging in the fraudulent practices alleged herein;

- b. ordering Defendant to maintain the basic network safeguards and any other antifraud measures that are necessary to protect consumers and limit consumer harm from fraudulent activity;
- c. ordering Defendant to provide an accounting of all New York consumers who reported losses to Defendant or its participating banks;
- d. ordering Defendant to pay restitution and damages to all injured New York consumers, whether known or unknown, at the time of the decision and order;
- e. ordering Defendant to disgorge all profits from the fraudulent practices alleged herein;
- f. awarding costs under CPLR 8303(a)(6); and
- g. granting such other and further relief as the Court deems just and proper.

Dated: August 12, 2025

Respectfully submitted,

LETITIA JAMES

Attorney General of the State of New York

By: 

Christian Reigstad

Assistant Attorney General

Christopher L. Filburn

Senior Enforcement Counsel

Bureau of Consumer Frauds & Protection

28 Liberty Street, 20th Floor

New York, New York 10005

Tel.: 212.416.8321

Email: christian.reigstand@ag.ny.gov

Tel.: 212.416.8303

Email: christopher.filburn@ag.ny.gov

Of counsel:

Jane M. Azia

Bureau Chief

Laura J. Levine

Deputy Bureau Chief

*Counsel for Plaintiff People
of the State of New York*