Benjamin R. Brunner (IL Bar # 6312432)
Benjamin Buchholz (DC Bar # 1780676)
Benjamin J. Clark (IL Bar # 6316861)
Christina Coll (CA Bar # 250712)
Alexis Christensen (DC Bar # 1723838)
Stephen Jacques (DC Bar # 464413)
Amanda Roberson (MN Bar # 0398511)
Noah Steimel (DC Bar # 1723832)
Samuel Taxy (IL Bar # 6333449)
1700 G Street, NW
Washington, DC 20552
Benjamin.Brunner@cfpb.gov, (681) 393-4915
Benjamin.Buchholz@cfpb.gov, (202) 445-8908
Benjamin.Clark@cfpb.gov, (202) 435-7871
Christina.Coll@cfpb.gov, (202) 435-7843
Alexis.Christensen@cfpb.gov, (202) 435-7301
Stephen.Jacques@cfpb.gov, (202) 435-7368
Amanda.Roberson@cfpb.gov, (202) 435-9447
Noah.Steimel@cfpb.gov, (202) 435-7985
Samuel.Taxy@cfpb.gov, (202)-435-7551

Attorneys for Plaintiff,
Consumer Financial Protection Bureau

UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF ARIZONA

Consumer Financial Protection Bureau, Plaintiff, v. Early Warning Services, LLC; Bank of America, N.A.; JPMorgan Chase Bank, N.A.; and Wells Fargo Bank, N.A. Defendants.	Case No: **COMPLAINT FOR PERMANENT INJUNCTION, MONETARY JUDGMENT, CIVIL PENALTY JUDGMENT, AND OTHER RELIEF**

The Consumer Financial Protection Bureau (Bureau) brings this action against Defendants Early Warning Services, LLC (EWS), Bank of America, N.A. (Bank of America), JPMorgan Chase Bank, N.A. (Chase), and Wells Fargo Bank, N.A. (Wells Fargo) (collectively, Defendants, and without EWS, Defendant Banks) and alleges as follows:

INTRODUCTION

1. Peer-to-peer platforms allow for the transfer of money almost instantaneously. Consumers can typically send money for free, making it an attractive method for transferring money to others. These types of payments first emerged in the late 1990s, but the number of users and transaction volume has grown exponentially in recent years.

2. By 2015, a number of peer-to-peer platforms had emerged. Several non-bank companies had rolled out platforms that were generating significant revenue and increasingly large customer bases. Bank of America, Chase, and Wells Fargo recognized this competitive threat and used EWS, a fintech and consumer reporting company owned by Defendant Banks with four other banks, to design and roll out their own peer-to-peer platform—Zelle.

3. The Zelle network is now offered by over 2,200 participating banks and credit unions. It has become one of the most widely available peer-to-peer payment networks in the United States, with more than 143 million users. In the first half of 2024, users transferred $481 billion across more than 1.7 billion transactions. In addition to being

part owners of EWS, Defendant Banks are the largest participating financial institutions in the Zelle network. In 2023, they accounted for 73% of activity on the Zelle network.

4. At its inception, Defendants focused on quickly bringing Zelle online to capture market share by leveraging their existing customer base and offering peer-to-peer money transfer services directly to those consumers. This rush to market was prioritized at the expense of consumers because Defendants have failed to institute effective anti-fraud measures for the network or otherwise comply with consumer financial protection laws.

5. 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.

6. The consequences of Zelle's shortcomings fell upon the shoulders of consumers. Since 2017, hundreds of thousands of consumers complained about being defrauded by Zelle users through various schemes. Yet consumers who went to their banks for help were largely denied relief, and some were even told to try getting their money back by contacting the person who had defrauded them.

7. Failures relating to fraud occurred at both the network and individual bank levels.

8. EWS operates the Zelle network and sets the rules that financial institutions agree to comply with in order to be part of the Zelle network. EWS also markets Zelle, and its marketing assured consumers that their transfers were safe and secure. But there was significant fraud on the network, and EWS has failed to take sufficient fraud-prevention actions. The network was set up in a way that made it easy for bad actors to access the system. And once those bad actors had access, EWS has failed to take basic steps to

detect or remove them from the network. EWS also has failed to stop transfers with unusual or suspicious characteristics that were likely to lead to consumer losses.

9. Since Zelle launched, each of the Defendant Banks has failed to prevent its own accountholders from using Zelle to defraud others, while also failing to protect other of its own accountholders from fraud when using Zelle. These failures were as basic as Defendant Banks not restricting the Zelle activity of their accountholders who engaged in Zelle fraud—or not sharing that information with EWS or other participating financial institutions on the Zelle network—which allowed those fraudsters to continue defrauding consumers across the Zelle network. And individual banks could have stopped Zelle transfers when there were indications of fraud, but they often failed to do so. Defendants failed to take steps to ensure consumers were protected from fraud, while nevertheless marketing Zelle as safe and secure.

10. Defendants' failures resulted in millions of complaints about Zelle fraud at these three banks alone, including complaints of over $290 million in fraud losses by 210,000 Bank of America customers, over $360 million in fraud losses by 420,000 Chase customers, and over $220 million in fraud losses by 280,000 Wells Fargo customers.

11. In addition to exposing consumers to Zelle fraud, Defendant Banks also violated Federal consumer financial law governing electronic fund transfers. Bank of America and Chase sent customers' transfers to the wrong recipients because of errors and inaccuracies in the Zelle Network Directory. And Defendant Banks did not conduct reasonable investigations when consumers came to them about certain fraudulent or otherwise erroneous Zelle transfers.

12. Defendants could have taken numerous steps, both individually and collectively, to prevent much of the harm to consumers. In addition to failing their customers, Defendants' actions and failures to act violated Federal consumer financial law.

13. The Bureau brings this action against Defendants under §§ 1054 and 1055 of the Consumer Financial Protection Act of 2010 (CFPA), 12 U.S.C. §§ 5564 and 5565 and § 918(a) of the Electronic Fund Transfer Act (EFTA), 15 U.S.C. § 1693o(a)(5) to obtain permanent injunctive relief, redress for affected consumers and an appropriate penalty, and to obtain all other appropriate relief for Defendants' violations of Federal consumer financial law.

JURISDICTION & VENUE

14. This Court has subject-matter jurisdiction over this action because it is brought under "Federal consumer financial law," 12 U.S.C. § 5565(a)(1), presents a federal question, 28 U.S.C. § 1331, and is brought by an agency of the United States, 28 U.S.C. § 1345.

15. The Court has personal jurisdiction over Defendants in this action because each Defendant conducts business in this District. In addition, EWS, which is owned in part by Defendant Banks, is headquartered in Arizona.

16. Venue is proper in this District under 12 U.S.C. § 5564(f) because each Defendant is located, resides, or is doing business in this District.

PARTIES

17. The Bureau is an independent agency of the United States charged with regulating the offering and provision of consumer financial products and services under Federal

consumer financial law. 12 U.S.C. § 5491(a). The Bureau has independent litigating authority to enforce Federal consumer financial law, including the CFPA, EFTA, and its implementing Regulation E. 12 U.S.C. §§ 5564(a)-(b), 5565, 5481(12)(C), (14).

18. EWS is a financial technology and consumer reporting company headquartered in Scottsdale, Arizona. It is co-owned by seven of the largest banks in the United States: Bank of America, Chase, Wells Fargo, Capital One, N.A., PNC Bank, N.A., Truist Bank, and U.S. Bank, N.A. EWS designed and operates the Zelle network and the Zelle App. In 2022, EWS had total revenue of approximately $429 million, about $200 million of which came from Zelle.

19. Bank of America is a national bank and subsidiary of Bank of America Corporation, headquartered in Charlotte, North Carolina. As of September 30, 2024, Bank of America had $2.57 trillion in consolidated total assets, making it an insured depository institution with assets greater than $10 billion within the meaning of 12 U.S.C. § 5515(a). As detailed below, in paragraphs 25 to 27, Bank of America exercises control over EWS and Zelle, and it is one of the largest participating financial institutions in the Zelle network. Bank of America maintains a significant retail banking operation in this District, with at least 107 branch locations in Arizona. Bank of America received at least 29,289 complaints from Arizona customers about its Zelle services from June 28, 2017, to August 23, 2023—74% of which related to fraud.

20. Chase is a national bank and subsidiary of JPMorgan Chase & Company with a main office in Columbus, Ohio. As of June 30, 2024, Chase had $3.58 trillion in consolidated total assets, making it an insured depository institution with assets greater

than $10 billion within the meaning of 12 U.S.C. § 5515(a). As detailed below, in paragraphs 25 to 27, Chase exercises control over EWS and Zelle, and it is the largest participating financial institution in the Zelle network. Chase maintains a significant retail banking operation in this District, with at least 193 branches in Arizona. Chase received at least 40,054 complaints from Arizona customers about its Zelle services from September 11, 2017, to December 7, 2023—66% of which related to fraud.

21. Wells Fargo is a national bank and subsidiary of Wells Fargo & Company headquartered in Sioux Falls, South Dakota. As of September 30, 2024, Wells Fargo had approximately $1.70 trillion in consolidated total assets, making it an insured depository institution with assets greater than $10 billion within the meaning of 12 U.S.C. § 5515(a). As detailed below, in paragraphs 25 to 27, Wells Fargo exercises control over EWS and Zelle, and it is one of the largest participating financial institutions in the Zelle network. Wells Fargo maintains a significant physical presence in the District, including 155 branches in Arizona. Wells Fargo received at least 43,571 complaints from Arizona customers about its Zelle services from Zelle's launch to May 26, 2023—71% of which related to fraud.

22. Defendants are "covered persons" under the CFPA because they offer and provide funds transmission and payment or other financial data processing services through the Zelle network, which are consumer financial products and services offered or provided "for use by consumers primarily for personal, family, or household purposes." 12 U.S.C. §§ 5481(5), (6)(A), 15(A)(iv), (vii).

23. Defendants Bank of America, Chase, and Wells Fargo, as national banks holding consumer deposit accounts, are also "financial institutions" subject to EFTA and Regulation E. 15 U.S.C. § 1693a(9); 12 C.F.R. § 1005.2(i).

FACTUAL ALLEGATIONS

I. BACKGROUND

A. Defendants Created Zelle, a Bank Peer-to-Peer System

24. Defendants launched Zelle in 2017 to compete with non-bank peer-to-peer payment networks such as Cash App and Venmo, and Zelle is now one of the country's most widely available peer-to-peer networks.

25. The network is owned and operated by EWS, which, in turn, is owned by seven major banks, including Defendant Banks.

26. Bank of America, Chase, and Wells Fargo each have one of seven votes on EWS's Zelle Management Committee (recently renamed the EWS Board), which makes ultimate decisions regarding the Zelle network. The management committee sets rules for the Zelle network which govern how banks and credit unions offer Zelle. These rules include how participating financial institutions must authenticate users seeking to enroll in the Zelle service; what information participating financial institutions must report to EWS about fraud and misdirected transfers; and when participating financial institutions must reimburse consumers for fraud or misdirected transfers. EWS is responsible for enforcing these rules and assessing fines if participating financial institutions fail to comply.

27. Each Defendant Bank has a representative on the EWS Enterprise Payments Advisory Board and Enterprise Payments Advisory Committee, whose roles,

respectively, are to provide strategic direction for the Zelle network and to provide advice and guidance in the execution of payment strategies.

28. Zelle is designed to be free, easy, and frictionless. Any person with a U.S.-based deposit account at one of the 2,200 participating financial institutions can register for Zelle. Consumers with a U.S.-based deposit account at non-participating financial institutions may register for Zelle with their debit cards on the Zelle App on their mobile phones.

29. To enroll in Zelle, a user is asked to provide an email address or mobile phone number, which is referred to as a "token" on the Zelle network. The user is then often asked to validate their token using a one-time passcode that is delivered to the phone number or email address that they selected. A user can enroll or register multiple email addresses or phone numbers to one bank account. A user can also enroll or register in Zelle at other participating financial institutions using different email addresses or phone numbers. A user can also reassign a particular email address or telephone number to a bank account at other participating financial institutions.

30. To send money to another user through the Zelle network, the sender inputs the recipient's email address or phone number—the recipient's token information—and the amount to be transferred. If the recipient's token is enrolled in Zelle, then the recipient receives the money at the bank account associated with that token. If the recipient's token is not enrolled in Zelle, a user can still send money to an email address or phone number and the recipient can access that money by enrolling with Zelle using that email address or phone number and linking it to a bank account.

31. Presently, a user's token—their email address or phone number—may be restricted by EWS or a participating financial institution. If a token is restricted, a sender's attempt to transfer money to that email address or phone number would not be completed.

32. Participating financial institutions, including Defendant Banks, may also pause or block specific transfers that they consider to be suspicious or risky, with each institution defining what constitutes a suspicious or risky transfer.

33. Consumers with deposit accounts at participating financial institutions, including the Defendant Banks, may access Zelle directly through their financial institution's mobile app or website.

34. Zelle is embedded in Defendant Banks' mobile apps; consumers cannot remove the Zelle function.

35. EWS maintains a Zelle Network Directory that matches registered tokens to the linked consumer, financial institution, and deposit account information.

36. After the sender completes the payment instructions, EWS matches the recipient token to its matched profile as listed in the Zelle Network Directory and sends a message to the receiving participating financial institution about the transfer. By agreement, the receiving institution makes the funds available in the recipient's account.

37. The sending and receiving financial institutions settle the day's Zelle transactions between themselves by the close of each day. But the sending and receiving financial institutions treat Zelle transfers as irrevocable at the time that the transfers are sent.

38. Even though Zelle is an interconnected network, [redacted]

39. As participating financial institutions in the Zelle network, each Defendant Bank [redacted]

B. From Its Start, Zelle Has Been an Attractive Vehicle for Fraud

40. From its launch, Zelle's marketing and branding, which EWS designed and Defendants implemented, exploited consumers' perceptions of the reliability and security of financial institutions and the assumption that the participating financial institutions will protect consumers from fraud.

41. Defendants have leaned into these consumer expectations and have widely marketed Zelle, such as through their websites, television, podcasts, radio, and on social media. Defendants encouraged consumers to use Zelle by promising that it is "safe" or "secure," and EWS even encouraged consumers to use Zelle to "pay it safe."

42. Notwithstanding these claims, since Defendants launched Zelle in 2017, a significant amount of fraud has occurred on the network.

43. Zelle is an attractive vehicle for fraud. It allows easy access for potential victims and bad actors alike. And funds are typically made available to the recipient immediately, making it easier for bad actors to quickly withdraw the funds.

44. Fraudsters can take advantage of Zelle's design and features, including the following:

a. Signup for Zelle is designed to be fast, easy, and frictionless. All users, including fraudsters, can generally register for Zelle if they have a deposit account and a US-based mobile phone number or email address.

b. To register a Zelle token, users must verify only that they have access to the email address or phone number (i.e., token) by entering a one-time passcode sent to that token from the participating financial institution. This level of authentication leaves consumers susceptible to fraud by bad actors. For example, in a scenario known as a token "takeover," a bad actor obtains a one-time passcode and token information from an unsuspecting consumer and reassigns that token to a deposit account in the bad actor's control. [redacted]

c. Zelle's use of email addresses and phone numbers as tokens fails to prevent fraud by making it difficult for senders to ascertain recipients' true identities. For example, this token design has allowed users to register misleading email addresses as Zelle tokens, including email addresses that appeared to be associated with the Defendant Banks.

d. At the point of transfer, network rules only require participating financial institutions to display limited information about the registered recipient—only the

recipient's first name—and not additional information that could alert the sender that the recipient is not who they purport to be.

e. Zelle allows transfers to unregistered tokens. This means that Zelle users can send money to email addresses and phone numbers that are not registered as a Zelle token. When this occurs, the unregistered recipient can access the money by later signing up for Zelle and linking their email address or phone number to their deposit account. In the case of unregistered tokens, no additional information beyond the recipient's email address or phone number is displayed.

f. [redacted]

g. Zelle allows a user to register up to five tokens to a deposit account at a single bank at the same time. This has allowed bad actors to use several different tokens—often with misleading email addresses—to evade detection and induce numerous consumers to send fraudulent transfers. For example, if a consumer filed a fraud claim against one token, a fraudster could defraud another consumer using a different token linked to a deposit account at the same bank. In the past, Zelle allowed even more tokens to be registered to a deposit account.

h. Zelle also allows users to switch the registration of a single token between different banks and, for years, register several tokens within a short period of time. This allowed users to associate and then disassociate numerous different tokens and switch tokens between participating financial institutions—a process referred

to as "flipping" tokens—to defraud consumers. For example, a fraudster could change their tokens across participating financial institutions and sign up for new tokens with new deposit accounts to avoid detection.

i. [redacted]

45. As a result of Zelle's design and features, including those above, the Zelle network is particularly susceptible to fraud, including unauthorized fraud and induced fraud.

46. Unauthorized fraud occurs when someone obtains access to a consumer's account or device and sends a transfer that the consumer neither authorizes nor benefits from. Such takeovers can occur in a variety of situations. For example, someone's phone might be stolen, hackers may take over a device remotely, or consumers may be tricked by an imposter into providing their account-login credentials. Bad actors exploit these scenarios to initiate unauthorized payments from the consumer's account.

47. Induced fraud occurs when a consumer is tricked into sending a transfer to someone under false pretenses. Common induced fraud schemes include: (1) a consumer duped into sending money in exchange for nonexistent goods or services; (2) a consumer duped into sending money as part of a fictitious romantic relationship; and (3) various imposter schemes such as when a bad actor seeks payment under the guise of being a business, financial institution, or government entity known to the consumer.

48. Me-to-Me schemes occur when a fraudster convinces a consumer to transfer money to a token that the consumer is led to believe is theirs when, in fact, the consumer is transferring the money to a token in the fraudster's control. In one common scenario, the fraudster convinces the consumer to share the one-time passcode provided by the consumer's financial institution, which allows them to re-assign the consumer's token to an account that the fraudster can access. The fraudster then convinces the consumer to send money to this token, which the consumer believes results in a transfer to the consumer's own deposit account.

49. Certain Me-to-Me schemes can flourish on the Zelle network because it allows transfers to be sent to unregistered tokens. When senders send money to unregistered tokens they do not see recipients' names, making it difficult for senders to ascertain recipients' true identities.

50. Each Defendant Bank typically does not provide credits to consumers' accounts for fraudulently induced transfers except in limited or one-off instances. Since mid-2023, the Zelle network has required participating financial institutions to reimburse a limited category of imposter schemes, but this covers a fraction of all induced fraud on the network.

C. Defendants Rushed to Launch Zelle Without Adequate Fraud Prevention Measures

51. Despite Defendants' prominent marketing of Zelle as "safe" and "secure," Defendants rushed Zelle to market without adequate and effective fraud prevention measures in place. Defendants devoted insufficient time and resources to understanding

the fraud-prevention measures needed for a network of Zelle's size, reach, and speed; and they conducted minimal fraud-prevention analyses, testing, and diligence before launch. Instead, Defendants focused on marketing and growing the Zelle user base. Ultimately, Defendants' collective failures left hundreds of thousands of consumer victims in their wake as Defendants played catch up over the course of several years to stem fraud.

52. Defendant Banks owned a digital payments company called clearXchange, which they sold to EWS in December 2015. Upon this acquisition, EWS announced its intention to "create the largest, most secure real-time payments ecosystems in the U.S." EWS planned to enable peer-to-peer payments and check deposits in the first quarter of 2016.

53. As Defendants began rolling out peer-to-peer payment technology, they pushed to rapidly launch, market, and brand Zelle in 2017, [redacted]

54. In the spring of 2017, Defendants continued to pursue a Zelle launch. They focused heavily on marketing and growing Zelle. [redacted]

55. By July 2017, Zelle had launched and was rapidly growing. Accompanying Zelle's rapid growth were significant fraud problems on the network. [redacted]

[redacted]

56. In 2018, Zelle continued to grow rapidly. Zelle reported that as of October 23, 2018, over the past year, Zelle processed more than 375 million transactions valued at $106 billion.

57. But with the uptick in consumer use of Zelle, Defendants saw that fraud continued to flourish on the network. [redacted]

58. Over the next six-plus years, EWS and Defendant Banks, including through their involvement on EWS committees and in their entity-specific materials, have repeatedly

identified numerous fraud prevention failures, including with respect to authenticating, verifying, and displaying recipient names, fraud reporting, monitoring transfers, and identifying and blocking bad actors across the network.

59. During this same period, EWS identified numerous anti-fraud measures, including measures related to consistent and enhanced information, reporting about recipients, and closing the accounts of bad actors when fraud is first reported against them. After identifying such measures, Defendants, however, took years to implement certain measures or have yet to implement other measures, almost eight years after Zelle's launch.

60. Defendants have failed to take timely, effective, and appropriate measures to prevent, detect, limit, and address Zelle fraud at both the network and entity level. Among other things, Defendants have failed to implement adequate authentication, verification, and registration requirements; to provide senders with sufficient information about recipients so that they can reduce the chance of transferring money to a bad actor; to implement measures to restrict known or suspected fraudsters; to pause or block suspicious or risky transfers; to report data necessary to prevent fraud; and to use relevant information provided by consumers in their complaints to detect and prevent further fraud.

61. Consumers had little reason to suspect that the Zelle network was rife with fraud. Consumers were not told about the lack of authentication and verification of Zelle users' token identities, including Zelle token names, email addresses, and other identifying information. Consumers were not told about the lack of fraud prevention measures,

including as to the lack of restriction of bad actors, lack of processes to pause or block suspicious transfers, and lack of information sharing about fraud. Instead, Defendants advertised the Zelle network to consumers using descriptions such as "safe," "secure," and "backed by the banks."

II. EWS, AS NEWORK OPERATOR, HAS FAILED TO PREVENT FRAUD AND HARMED CONSUMERS

62. Since the 2017 launch, EWS has promoted Zelle as "safe" and "secure," regardless of where consumers bank. EWS ads have also promised that Zelle is "[f]ast, safe, and easy."

63. Early EWS television advertisements airing from 2017 through 2018 suggested that consumers could buy football playoff tickets safely with Zelle because "it was backed by the banks so you know it's secure."

64. During the COVID-19 pandemic, EWS created ads touting Zelle as a "fast," "safe," and "contact-free" way to transfer money and that consumers could enroll in Zelle through their banking app.

65. But in fact, EWS has failed to take timely, effective and appropriate measures to prevent, detect, limit, and address Zelle fraud because, among other failures, it has: (1) implemented limited authentication, verification, and registration requirements which permitted bad actors onto the Zelle network; (2) provided limited information to consumers about the identity of the transfer recipients; (3) failed to provide certain risk-related information to—and, when available, requiring its use by—participating financial institutions for their use when pausing or blocking suspicious or risky transfers; (4) failed

to suspend or restrict fraudsters from using Zelle; (5) failed to require participating financial institutions to report timely and accurate information about fraud—and even when it instituted such reporting requirements, it failed to ensure participating financial institutions complied with such requirements; and (6) failed to adequately monitor compliance with the network rules.

66. As a result, Zelle users lost hundreds of millions of dollars to fraud. Moreover, Zelle's users consistently complained to EWS and participating financial institutions about fraud on the network, the Zelle network's failure to protect them, and the Zelle network's lack of fraud protections. Despite these complaints, EWS has failed to take timely, effective, and appropriate measures to prevent, detect, limit, and address Zelle fraud.

A. EWS's Failures Relating to Authentication and Identification Requirements

67. EWS has limited network rules relating to authenticating Zelle users' identities and verifying users' access to Zelle token information, and [redacted]

68. EWS created a consumer sign-up process that was intentionally fast and frictionless, which allowed users to register for a Zelle token if they had a bank account and U.S.-based mobile phone number or email address and could access the email or mobile device to receive and enter a one-time passcode. [redacted]

[redacted]

69. [redacted]

[redacted]

70. EWS also allows users to register multiple Zelle tokens with a single participating financial institution and use Zelle at various participating financial institutions. [redacted]

[redacted] By reassigning tokens to new deposit accounts, fraudsters can gain control of a victim's token and reassign it to the fraudster's account.

71. EWS allows a user to enroll multiple unique tokens (i.e., unique email addresses or phone numbers) with a single participating financial institution in a short period of time. Token flipping can lead to fraud.

72. [redacted]

[redacted]

73. [redacted]

[redacted]

74. From 2018 until April 2023, network rules allowed users to associate up to 20 unique tokens per participating financial institution. After April 2023, network rules limited users to associate up to five tokens per participating financial institution.

75. [redacted]

76. EWS has also failed to require the use of specific mechanisms for participating financial institutions to identify and prevent a user from enrolling in Zelle using a suspicious email token until 2023.

77. For example, bad actors repeatedly signed up for tokens using email addresses that falsely indicated that the user was a large business or government entity. Network rules, however, allow only individuals and small businesses to receive funds.

78. Zelle tokens using emails impersonating a legitimate entity, including "Zelle" and some of Defendant Banks, were often the subject of numerous fraud complaints.

79. After years of consumers complaining about imposter and other fraud schemes, [redacted]

B. EWS's Failures Relating to Providing Readily Available Recipient Information to Consumers

80. EWS did not require participating financial institutions to provide senders with readily available information about recipients, including recipients engaged in imposter

and Me-to-Me schemes, at the point of transfer. As described in paragraph 44, such information could have alerted consumers that recipient fraudsters were not who they claim to be.

81. When EWS first launched Zelle, it did not require participating financial institutions to provide senders with any identifying information about the recipient other than their token.

82. In September 2018, EWS required participating financial institutions to display the recipient's first name at the point of transfer. But since then, EWS has not required participating financial institutions to display any additional identifying information that would help senders identify recipients, such as the recipient's last name, the age of the token, or amount of time the user was on Zelle.

83. EWS also allows users to transfer money to unregistered tokens, which are email addresses or U.S.-based mobile phone numbers not associated with a deposit account in the Zelle network. In those circumstances, a Zelle user can transfer money to the recipient's phone number or email address, although no recipient name would be displayed. A recipient then has between 14 and 20 days to receive the payment by enrolling in Zelle through a participating financial institution, or by using their Visa or Mastercard debit card to enroll.

84. [redacted] For example, in a common Me-to-Me scheme, the bad actor convinces the consumer to initiate or complete a transfer to an unregistered token, which displays no name, and the bad actor misrepresents that the token is

connected to a special account at the bank for helping consumers when the token is in fact connected to the bad actor's own account. The lack of a user first name displayed during the transaction helps facilitate the fraud. To date, EWS continues to permit users to transfer money to unregistered tokens.

85. EWS's failure to implement network rules requiring participating financial institutions to display readily available information about recipients' identities increases the risk of fraud and makes it more difficult for consumers to avoid transferring funds to bad actors.

C. EWS's Failures Relating to Blocking Suspicious or Risky Transfers

86. Fraudulent transfers often exhibit unusual or suspicious characteristics that enable banks to detect and prevent consumer losses.

87. [redacted]

88. [redacted]

89. [redacted]

[redacted]

90. [redacted]

91. [redacted]

92. [redacted]

D. EWS's Failures Relating to Suspending or Restricting Bad Actors from Zelle

93. [redacted]

94. [redacted]

95. [redacted]

96. [redacted]

97. [redacted]

98. [redacted]

99. [redacted]

100. [redacted]

101. [redacted]

102. [redacted]

[redacted]

[redacted]

E. EWS's Failures Relating to Fraud Reporting

103. EWS has failed to require participating financial institutions to report timely and accurate information about fraud. And even when EWS instituted fraud reporting requirements, it failed to ensure participating financial institutions complied with such requirements.

104. At Zelle's launch, EWS required participating financial institutions to report transactions disputed as unauthorized and confirmed or closed for fraud. EWS's definition of fraud, however, did not include induced fraud, which occurs when a consumer is tricked into sending a transfer to someone under false pretenses, such as in exchange for nonexistent goods or services or as part of a fictitious romantic relationship.

[redacted]

105. [redacted]

106. Even then, many participating financial institutions have failed—sometimes repeatedly—to meet these reporting obligations.

107. Since Zelle's launch, the network rules have required the prompt reporting of fraud (excluding induced fraud). In practice, however, EWS allowed participating financial institutions to report fraud to EWS long after it occurred.

108. EWS knew that its failures to require and receive timely fraud reports led to increased fraud risk for consumers. For example:

a. [redacted]

b. [redacted]

c. [redacted]

d. [redacted]

e. [redacted]

109. [redacted]

F. EWS's Failures to Adequately Monitor Participating Financial Institutions for Network Rule Compliance

110. EWS has failed to adequately monitor for compliance and enforce the Zelle network rules.

111. Since Zelle's launch, EWS has failed to devote sufficient resources to enforce Zelle network rules. [redacted]

112. EWS created a formal Fraud Monitoring Program in or around April 2021, almost four years after it launched Zelle. [redacted]

113. EWS knew that participating financial institutions were repeatedly violating network rules that, though insufficient, were designed to prevent, detect, limit, and address fraud. For example:

a. [redacted]

b. [redacted]

c. [redacted]

d. [redacted]

e. [redacted]

114. The network rules state that EWS will impose fees on participating financial institutions when it determines that they have failed to comply with certain network rules. [redacted]

115. [redacted]

116. [redacted]

117. [redacted]

[redacted]

III. BANK OF AMERICA HAS FAILED TO PROTECT CONSUMERS FROM ZELLE FRAUD

118. Early feedback from Bank of America customers reflected that they felt one of Zelle's most important features was the network's perceived security. Bank of America also observed that consumers expected their bank to get involved, provide guidance, and protect them from bad actors.

119. From 2017 through at least October 2020, Bank of America promoted as a security feature of Zelle that consumers "would not be liable for fraudulent transactions." At various points, Bank of America included this or similar language about consumers' liability for fraudulent transactions in promotional emails encouraging accountholders to use Zelle, in the mobile app's in-app flow, on its Frequently-Asked-Questions webpage, and on the bank's Zelle landing webpage.

120. On the sign-out page of its website in at least 2020, Bank of America displayed an advertisement for Zelle that highlighted the words: "Fast," "Safe," "Easy," and "Free." Underneath the word "Safe," the website stated, "Authentication and monitoring features mean peace of mind."

121. Bank of America's sign-in for its website and mobile app encouraged users to send money to hairstylists, landscapers, and other workers using Zelle. Bank of America ran multimedia campaigns telling consumers that Zelle is "the fast, safe and easy way to pay for everything you need on the go." Bank of America also encouraged consumers to use Zelle to pay "almost anyone."

122. In fact, Bank of America has failed to take timely, effective and appropriate measures to prevent, detect, limit, and address Zelle fraud because, among other failures, it has: (1) implemented only limited authentication, verification, and registration requirements which permitted bad actors onto the Zelle network; (2) provided limited information to consumers about the identity of the recipient; (3) failed to pause or block suspicious or risky transfers; (4) failed to suspend or restrict fraudsters from using Zelle; (5) failed to timely report fraud-related information to EWS; and (6) failed to use relevant information from consumers' complaints about fraud to prevent future consumer harm.

123. As a result of its failures, Bank of America customers and other Zelle users lost hundreds of millions of dollars.

124. Moreover, Bank of America's customers consistently complained to Bank of America about fraud on the network, Bank of America's failure to protect them, and Bank of America's lack of fraud protections. Despite these complaints, Bank of America has failed to take timely, effective, and appropriate measures to prevent, detect, limit, and address Zelle fraud.

A. Bank of America's Failures Relating to Authenticating and Registering Zelle Users

125. Bank of America performed only limited identity authentication before allowing users to join the network or reassign their token to a different bank account. Bank of America's failures increased fraud risk for Bank of America customers and Zelle users across the network.

126. Bank of America often failed to comply with the minimal Zelle network requirements for authentication at token enrollment.

127. Network rules permit users to register U.S.-based mobile phone numbers as tokens. Users are not allowed to register voice-over-internet phone (VoIP) numbers and international phones, which are associated with higher fraud rates, as tokens.

128. In spite of these prohibitions, through at least September 2019 and May 2020, respectively, Bank of America permitted users to register VoIP numbers and Canadian mobile phone numbers as tokens, which violated the then-operative Zelle network rules.

129. [redacted]

130. [redacted]

[redacted]

131. Bank of America also permitted bad actors to repeatedly flip and change tokens, which increased the risk of Zelle fraud.

132. [redacted]

133. [redacted]

134. Bank of America has also failed to implement simple and basic authentication measures despite being aware of widespread fraud on Zelle.

135. [redacted]

136. Bank of America also failed to implement mechanisms for identifying and suspending suspicious email tokens at signup until 2023.

137. [redacted]

138. These tokens were in turn used to fraudulently induce transfers from consumers with Bank of America accounts. When consumers complained, Bank of America denied their claims.

B. Bank of America's Failures Relating to Providing Readily Available Recipient Information to Consumers

139. Bank of America has not provided readily available information about recipients to its sending accountholders at the point of transfer: this lack of information increased the risk of fraud, including through imposter and Me-to-Me schemes. Such information could have alerted consumers that recipient fraudsters were not who they claimed to be.

140. When Zelle was first implemented at the bank, senders could not see any identifying information about the recipient.

141. Beginning in September 2018, the bank began displaying recipients' first names to comply with a Zelle network rule requiring sending banks to display the first name associated with the accountholder in the Zelle Network Directory.

142. [redacted]

[redacted]

143. [redacted]

144. Bank of America did not consistently provide the last name of the recipient at the point of transfer until November 2022, at which point Bank of America also began alerting consumers when a recipient token was newly registered. Bank of America does not display other information to which it has access, such as whether the recipient has a consumer or business account, that would allow a consumer to better assess the risk of sending a payment.

C. Bank of America's Failures Relating to Blocking Suspicious or Risky Transfers

145. Bank of America uses a fraud detection system to monitor, pause, and block transfers based on fraud risk, including transfers that exhibit unusual or suspicious activity based on information about the sender, recipient, and transfer.

146. [redacted]

147. [redacted]

148. [redacted]

149. [redacted]

150. Similarly, Bank of America has received over 8,000 complaints about transfers where the recipient's name, as input by the sender, contained suspicious phrases such as "refund," "Bank of America," and "tickets." [redacted]

D. Bank of America's Failures Relating to Suspending or Restricting Bad Actors from Zelle

151. Bank of America's own customers have been the subject of multiple complaints about fraud or exhibited highly unusual or suspicious behavior, such as large-dollar transfers, rapid movement of funds, and flipping tokens. Yet, for years, the bank has

failed to restrict the tokens or suspend the accounts of these bad actors, permitting them to continue to victimize consumers across the Zelle network.

152. [redacted]

153. [redacted]

154. [redacted]

a. [redacted]

b. [redacted]

155. [redacted]

156. [redacted]

157. [redacted]

E. Bank of America's Failures Relating to Timely Reporting Fraud-Related Information

158. Bank of America failed to consistently and timely report information about fraud to EWS even though the network rules require such fraud reporting.

159. [redacted]

[redacted]

160. [redacted]

161. [redacted]

162. [redacted]

F. Bank of America's Failure to Use Consumer Complaint Information to Prevent or Detect Fraud

163. Consumers regularly complain to Bank of America about fraud on the Zelle network, but the bank has failed to effectively use such information to prevent or detect fraud.

164. When a consumer files a complaint with Bank of America, an intake staffer asks a series of automatically generated questions to classify the complaint and gather other details about the transfer from the consumer.

165. [redacted]

166. [redacted]

167. [redacted]

168. [redacted]

169. [redacted]

170. [redacted]

171. When Bank of America determined that it could not claw back the funds from the fraudster's account, it typically instructed the consumer to resolve the claim by working it out with the fraudster. Bank of America did not assist the consumer in contacting the recipient or provide any additional identifying information and otherwise typically did not pay the consumer's claim.

172. [redacted]

G. Bank of America's Failures Have Caused Significant Consumer Harm

173. As a result of Bank of America's failures to take timely, effective, and appropriate measures to prevent, detect, limit, and address Zelle fraud from the network's inception through the present, including the specific failures above, consumers have suffered significant harm.

174. Through August of 2023, Bank of America received more than 324,000 complaints from its accountholders about potentially fraudulently induced transfers for which it did not provide a credit for the amount of the transfer, for a total of over $207 million.

175. Through August of 2023, Bank of America received more than 161,000 complaints from its accountholders about potentially unauthorized transfers for which it did not provide a credit for the amount of the transfer, for a total of over $85 million.

176. Through August of 2023, Bank of America received more than 1,200 complaints from its accountholders about potential Me-to-Me schemes for which it did not provide a credit for the amount of the transfer, for a total of over $1 million.

177. In total, through August of 2023, hundreds of thousands of Bank of America customers have complained to Bank of America about $293 million in fraud on the Zelle network and have not been reimbursed.

H. Bank of America Was Aware that Consumers Felt Misled about Zelle's Security

178. Bank of America has consistently received consumer complaints that showed that consumers were unable to recognize and avoid harms from Zelle fraud.

179. The bank's customers have repeatedly expressed frustration with Zelle's lack of security. Among other things, Bank of America customers have repeatedly raised the following types of issues in their complaints:

a. "I was unfamiliar with the app, but felt confident in it when it was *literally included* within my Bank of America app. The email address for the recipient is listed as 'verified.'"

b. "I used Zelle because it shows on my bank's mobile page and I felt this was supported by Bank of America and safe. …Why does Bank of America advertise this Money transfer service if it is not safe. I am a Platinum customer at BOA and

I feel they should refund the $350 and put Huge Warnings on the web page to warn against this type of fraud."

c. "ZELLE is promoted constantly by Bank of America as a safe and secure way to transfer funds. [] I received no warnings when making the transaction that the 'seller' or 'scammer' may not be a legitimate account holder."

d. "I made the transaction through the BoA app and I thought it was covered from fraud protection like other transactions because it is part of the same app and clearly branded on the front page. I was misled into thinking [Z]elle was owned or is a part of BoA or at the very least should be covered from fraud."

IV. CHASE HAS FAILED TO PROTECT CONSUMERS FROM ZELLE FRAUD

180. When Chase conducted market research, it found that its customers viewed Zelle as secure because of its association with the bank. A consumer interviewed by Chase explained, "[w]hen [Zelle] is linked to Chase, it gives me confidence that my transaction will be protected." Chase also found that, in consumers' views, "bank-backed/endorsement means secure" and that Zelle's association with Chase provided it with a "trust halo."

181. Chase's advertisements for Zelle have described the product as "[s]ecure," and explained that Zelle transfers could be sent to "practically anyone," "virtually anyone," or "almost anyone."

182. From 2019 through 2020, Chase's Zelle advertisements featured a photo of a woman sending a Zelle transfer and informed consumers, "[m]ultiple security checks

have been added to make sure you're sending and receiving money to/from the right person."

183. In fact, Chase has failed to take timely, effective, and appropriate measures to prevent, detect, limit, and address Zelle fraud because, among other failures, it has (1) implemented only limited authentication, verification, and registration requirements which permitted bad actors onto the Zelle network; (2) provided limited information to consumers about the identity of the recipient; (3) failed to pause or block suspicious or risky transfers; (4) failed to suspend or restrict fraudsters from using Zelle; (5) failed to timely report fraud-related information to EWS; and (6) failed to use relevant information from consumers' complaints about fraud to prevent future consumer harm.

184. As a result of its failures, Chase consumers and other Zelle users lost hundreds of millions of dollars. Moreover, Chase's customers consistently complained about fraud on the network, Chase's failure to protect consumers, and Chase's lack of fraud protections. Despite these complaints, Chase has failed to take timely, effective, and appropriate measures to prevent, detect, limit, and address Zelle fraud.

A. Chase's Failures Relating to Authenticating and Registering Zelle Users

185. Chase has performed only limited identity and token authentication of its accountholders who used Zelle, which has permitted bad actors to operate on the Zelle network.

186. When Chase accountholders seek to enroll in the Zelle service, Chase has sent a one-time passcode to the email address or phone number provided by the accountholder to confirm their access to the token. Chase has not required any further authentication of

prospective Zelle users at enrollment, and tokens could be enrolled or reassigned to different Chase accounts by providing a one-time passcode sent to the token.

187. Chase has not limited the number of times a user can change the token associated with their deposit account, [redacted]

188. [redacted]

189. [redacted]

190. [redacted]

191. Chase has also failed to implement effective mechanisms for identifying and suspending suspicious email tokens at signup. [redacted]

[redacted]

192. [redacted]

[redacted]

B. Chase's Failures Relating to Providing Readily Available Recipient Information to Consumers

193. Chase has not provided readily available information about recipients to the sending accountholder at the point of transfer, and this lack of information increased the risk of fraud, including through imposter and Me-to-Me schemes.

194. At the launch of Zelle, Chase did not display recipient information (such as the recipient's name) to the sender at the point of transfer.

195. In late summer or early fall of 2018, Chase, in response to a new Zelle network requirement, began displaying the first name associated with recipient tokens in the Zelle Network Directory to the sender at the point of transfer.

196. Initially, the first name was displayed once, just before senders entered a recipient token for the first time, when a recipient had been inactive for more than six months, or when Chase identified a change in token ownership.

197. [redacted]

198. [redacted]

199. In late 2020, Chase also began displaying the first name associated with recipient tokens in the Zelle Network Directory any time Chase customers entered a token to send a Zelle transfer and throughout the process of sending a transfer.

200. Chase did not begin displaying the last name associated with recipient tokens in the Zelle Network Directory until May 2023 at the earliest.

201. Chase has not displayed other information that would allow a consumer to better assess the risk of sending a payment, such as whether the recipient has a consumer or business account, despite Chase having access to that information.

C. Chase's Failures Relating to Blocking Suspicious or Risky Transfers

202. While Chase has used a fraud detection system to pause or block various kinds of transfers that have presented an elevated risk of fraud, including Zelle transfers, that system has been inadequate for protecting consumers from the specific fraud risks presented by the Zelle network. [redacted]

203. [redacted]

204. [redacted]

205. [redacted]

206. [redacted]

[redacted]

207. [redacted]

[redacted]

D. Chase's Failures Relating to Suspending or Restricting Bad Actors from Zelle

208. Chase has failed to timely suspend or restrict suspected or known bad actors and, thus, to stop them from using Zelle to continue perpetrating fraud.

209. [redacted]

[redacted]

210. [redacted]

[redacted]

211. [redacted]

E. Chase's Failure to Timely Report Fraud-Related Information

212. Chase has failed to report basic information that EWS and other participating financial institutions could have used to prevent or limit fraud on the network.

213. [redacted]

214. [redacted]

215. [redacted]

216. [redacted]

217. [redacted]

218. [redacted]

219. [redacted]

F. Chase's Failure to Use Consumer Complaint Information to Prevent or Detect Fraud

220. Chase received hundreds of thousands of complaints about fraud related to Zelle, but it has failed to properly use the information from these complaints to detect and prevent further fraud.

221. Chase has encouraged consumers to file claims, but when consumers did so, [redacted]

222. [redacted]

223. [redacted]

224. Chase's handling of induced fraud claims has led to further fraud-prevention failures, including delayed identification of repeat bad actors and emerging fraud patterns.

G. Chase's Failures Caused Significant Consumer Harm

225. As a result of Chase's failure to take timely, effective, and appropriate measures to prevent, detect, limit, and address Zelle fraud, including the specific failures above, consumers have suffered significant harm.

226. Through December 2023, over 1,000 Chase accountholders complained of fraudulent inducement through Me-to-Me schemes and did not receive a credit for the amount of the transfer, for a total of over $1.1 million. In addition, at least another

320,000 Chase accountholders complained of fraudulent inducement through other schemes and did not receive a credit for the transfer, for a total of over $251 million.

227. [redacted] Instead, Chase has typically told consumers that they could resolve the claim by working it out with law enforcement or the recipient (i.e., the fraudster), but has not provided consumers with other information about the recipient, the recipient's account, or the recipient's Zelle token.

228. Finally, Chase should have been aware that its failures were likely to result in preventable consumer harm. [redacted]

H. Chase Was Aware that Consumers Felt Misled about Zelle's Security

229. Chase has consistently received consumer complaints that have shown that consumers were unable to recognize and avoid harms from Zelle fraud.

230. The bank's customers have repeatedly expressed confusion and frustration with Zelle's lack of security. Among other things, Chase customers have repeatedly raised the following types of issues in their complaints:

a. "My chase bank app has a zelle option. I used it bc its on CHASE APP as an option to pay…. Chase is supposed to be a secure safe app. If so why do they offer zelle as a payment??? When if fraud there's zero help?"

b. "I went online, logged into our Chase account and saw Zelle listed as an option to use for making payments so we thought Zelle had to be secure, right??.... Scammers point out that Zelle is on the Chase website so its gotta be safe, right?!!"

c. "I trusted that Chase would protect my purchases or payments so i used Chase's payment program…. I also feel that Chase was not clear in their lack of customer protections and should have a brief disclaimer before a transaction is submitted saying they do not reimburse, scam or not."

V. WELLS FARGO HAS FAILED TO PROTECT CONSUMERS FROM ZELLE FRAUD

231. Wells Fargo has marketed Zelle as "safe" and "secure." For example, ads have stated: "Make Zelle your go-to for sending money. Next time you want to send money, try Zelle. It's fast, safe, and easy. Plus, it's free in your Wells Fargo Mobile app," and "With Zelle, it's fast, safe, and easy to send money to friends, family, and even some businesses. Plus, it's already in your Wells Fargo app."

232. An early consumer complaint to Wells Fargo highlighted consumers' belief that Zelle was secure: "The scammer assured me that the transaction was secure because I was using the Wells Fargo app. It is reasonable to assume that bank transactions are secure against fraud, and the design of the Wells Fargo app does not make it clear that

Zelle is a distinct, non-secure service. … I would not have fallen victim to this scam but for the fact that this service is contained within the Wells Fargo app alongside normal banking services, and the fact that no noticeable effort is made to inform the user that Zelle is a distinct service without normal banking protections."

233. Wells Fargo also reinforced the safety of Zelle on the Wells Fargo mobile app in the Zelle enrollment process. From 2019 through 2021, the initial page to enroll in Zelle on the Wells Fargo application read: "Move money in the moment. Simply and securely – with lots of people you know." Starting in 2022, the initial-enrollment page read "Send Money with Zelle: Send money safely to people and businesses you know, in just a few taps." Accessing Zelle through a browser on mobile phones led to a similar enrollment message: "Zelle: Move money in the moment. Simply and securely – with people and eligible businesses you trust."

234. Wells Fargo made similar representations on its website. There, from at least June 2018 to July 2022, the initial Zelle home page that allowed consumers to initiate a transfer read, "Send Money with Zelle: Send and receive money securely – all you need is an email address or mobile number." And the website currently states: "Whether it's across the hall or across the country, you can safely send and receive money with friends, family, and others with a U.S. bank account."

235. In fact, Wells Fargo has failed to take timely, effective, and appropriate measures to prevent, detect, limit, and address Zelle fraud because, among other failures, it has (1) implemented only limited authentication, verification, and registration requirements, which permitted bad actors onto the Zelle network; (2) provided limited information to

consumers about the identity of the recipient; (3) failed to pause or block suspicious or risky transfers; (4) failed to suspend or restrict fraudsters from using Zelle; (5) failed to timely report fraud-related information; and (6) failed to use relevant information from consumers' complaints about fraud to prevent future consumer harm.

236. As a result of its failures, Wells Fargo customers and other Zelle users lost hundreds of millions of dollars. Moreover, Wells Fargo's customers have consistently complained to Wells Fargo about fraud on the network, Wells Fargo's failure to protect them, and Wells Fargo's lack of fraud protections. Despite these complaints, Wells Fargo has failed to take timely, effective, and appropriate measures to prevent, detect, limit, and address Zelle fraud.

A. Wells Fargo's Failures Relating to Authenticating and Registering Zelle Users

237. Wells Fargo performs only limited identity authentication of its accountholders who use Zelle, which allows bad actors to operate on the Zelle network.

238. When an existing accountholder signs up for Zelle, Wells Fargo performs limited or no additional authentication beyond confirming access to the token by issuing a one-time passcode to the user's token (their phone number or email address), which the user would have to verify to use Zelle with that token.

239. For much of Zelle's existence, Wells Fargo has failed to implement basic authentication measures to reduce fraud. [redacted]

[redacted]

240. [redacted]

241. [redacted]

242. Through March 2022, Wells Fargo permitted accountholders to send money using Zelle without registering a token at all. As explained above, this put consumers at greater risk for Me-to-Me schemes because bad actors could register the sender's unregistered phone number or email address to their own account and then persuade the consumer to transfer funds to the now-registered token.

243. [redacted]

244. Wells Fargo also failed to implement mechanisms for identifying and suspending suspicious email tokens at signup. [redacted]

B. Wells Fargo's Failures Relating to Providing Readily Available Recipient Information to Consumers

245. Wells Fargo does not provide readily available information about recipients to the sending accountholder at the point of transfer that would allow consumers to identify fraud more easily. This lack of information increased the risk of fraud, including through imposter and Me-to-Me schemes. The bank's various attempts to provide more information to consumers over the years have been de minimis and inconsistent.

246. In or around October 2018, Wells Fargo began displaying the first name of recipients who were receiving funds from a consumer for the first time. But it did not always do so until mid-2020.

247. Wells Fargo did not proactively alert senders when the recipient's name, as entered by the sender, differed from what was recorded in the Zelle Network Directory until 2022.

C. Wells Fargo's Failures Relating to Blocking Suspicious or Risky Transfers

248. Wells Fargo has known that its fraud detection and prevention protocols were insufficient from the start. [redacted]

249. [redacted]

250. [redacted]

D. Wells Fargo's Failures Relating to Suspending or Restricting Known Bad Actors from Zelle

251. Wells Fargo also has failed to adequately suspend or restrict the tokens or accounts of thousands of its own accountholders about whom it had received multiple complaints, including many with five or more complaints.

252. [redacted]

[redacted]

E. Wells Fargo's Failure to Timely Report Fraud-Related Information

253. At times since Zelle's launch, Wells Fargo often failed to timely report, or report at all, information about fraud to EWS in violation of the network rules.

254. [redacted]

255. [redacted]

256. [redacted]

257. [redacted]

258. [redacted]

[redacted]

F. Wells Fargo's Failure to Use Consumer Complaint Information to Prevent or Detect Fraud

259. Wells Fargo has failed to use information from consumer complaints to prevent or detect fraud.

260. [redacted]

261. [redacted]

262. [redacted]

263. [redacted]

264. When the bank determines that it cannot claw back the funds from a bad actor's account, it often has directed the consumer to resolve the claim by contacting the bad actor using the bad actor's token information.

265. The design of the bank's complaint intake process has contributed to Wells Fargo's failure to act quickly to retrieve or secure fraudulently transferred funds. When a consumer discovers that they have been defrauded seconds or minutes after a transfer occurs, they are unable to immediately report the fraud using an online complaint. Instead, they must contact the bank by mail, in-person, or by phone, where they may encounter wait times of over an hour. Any delay increases the likelihood that the bank will not be able to claw back the funds.

266. Wells Fargo's handling of induced fraud claims has caused delays in identifying bad actors and responding to fraud patterns.

G. Wells Fargo's Failures Caused Significant Consumer Harm

267. As a result of Wells Fargo's failure to take timely, effective, and appropriate measures to prevent, detect, limit, and address Zelle fraud, including the specific failures above, consumers suffered significant harm.

268. From launch through May 2023, more than 160,000 Wells Fargo accountholders have complained about potential fraudulent inducement and did not receive a credit for the amount of the transfer, for a total of over $105 million.

269. From launch through May 2023, more than 120,000 Wells Fargo accountholders complained about potentially unauthorized fraud and did not receive a credit for the amount of the transfer, for a total of over $110 million.

270. From launch through May 2023, more than 3,900 Wells Fargo accountholders complained of fraudulent inducement through Me-to-Me schemes and did not receive a credit for the amount of the transfer, for a total of over $5 million.

H. Wells Fargo Was Aware that Consumers Felt Misled about Zelle's Security

271. Wells Fargo has consistently received consumer complaints that showed that consumers were unable to recognize and avoid harms from Zelle fraud. Most of the losses associated with those complaints, more than $220 million, were never reimbursed by the bank.

272. The bank's customers have repeatedly expressed frustration with Zelle's lack of security. Among other things, Wells Fargo customers have repeatedly raised the following types of issues in their complaints:

a. "ZELLE IS ON THEIR ONLINE BANKING APP! If they do not cover fraud on Zelle purchases then they should remove it from their Wells Fargo App. That is VERY misleading!"

b. "Wells Fargo promotes the use of Zelle for sending money. They even have a specific tab to use Zelle in their mobile app, [and] the entire transaction is done via the Wells Fargo mobile app. … Wells Fargo refused to assist in any way. I discovered via a subpoena that the recipient of my 5 Zelle payments was also a Wells Fargo customer & the money was sent to 'her' Wells Fargo account. Wells Fargo again refused to assist or provide any status updates. To my knowledge, they did absolutely nothing. … Instead, they promote someone using a payment app (Zelle) as a fraud platform."

VI. DEFENDANT BANKS HAVE FAILED TO PROVIDE PROTECTIONS REQUIRED UNDER EFTA TO ZELLE USERS

273. EFTA and its implementing Regulation E specify required procedures for resolving errors related to electronic fund transfers (EFTs).

274. Under EFTA and Regulation E, when a consumer submits an oral or written notice involving an EFT to a financial institution that qualifies as a "Notice of Error" under Regulation E, the financial institution must conduct a reasonable investigation of the consumer's notice, which includes reviewing any relevant information from an institution with whom the financial institution has an agreement. 12 C.F.R. § 1005.11.

275. A reasonable investigation of a Notice of Error includes a review of any relevant information in the financial institution's own records, as well as any relevant information of third parties with which the institution has an agreement. Relevant information may include the consumer's payment instructions, as well as any other information appropriate to resolve the claim in the financial institution's possession or control, such

as (1) transaction records for the transfer, (2) the transaction history of the particular account for a reasonable period of time immediately preceding the allegation of error, and (3) the location of either the transaction or the recipient in question relative to the consumer's place of residence and habitual transaction area. 12 C.F.R. § 1005.11(c)(4); 12 C.F.R. § 1005.11 Supp. I, cmt. 11(c)(4).

276. Errors include incorrect transfers and unauthorized transfers. 12 C.F.R. § 1005.11(a)(1). An unauthorized transfer (Unauthorized Transfer) from a consumer's account is one initiated by a person other than the consumer without actual authority to initiate the transfer and from which the consumer receives no benefit. Unauthorized Transfers include transfers initiated by a person who obtained the consumer's access device through fraud or robbery. 12 C.F.R. § 1005.2(m); 12 C.F.R. § 1005.11 Supp. I, cmt. 2(m).

277. If a financial institution determines that an Unauthorized Transfer or other error has occurred, it must correct the error by, if appropriate, providing a credit to the consumer's account. 12 C.F.R. § 1005.6(b); 12 C.F.R. § 1005.11(a)(1) and (c); 12 C.F.R. § 1005.11 Supp. I, cmt. 11(c).

278. Transfers through Zelle are EFTs because they are transfers of funds initiated through a computer or telephone for the purpose of or authorizing a financial institution to debit or credit a consumer's account. 12 C.F.R. § 1005.3(b)(1).

279. Defendant Banks, along with other participating financial institutions, have an agreement through EWS to participate in Zelle. This agreement includes sending and

receiving transfers from each other, and honoring senders' payment instructions for Zelle transfers.

280. Under Regulation E, an oral or written notice of error (Notice) generally must (1) be received by an institution no later than 60 days after it sends a periodic statement on which the alleged error is first reflected, (2) enable the institution to identify the consumer's name and account number, and (3) indicate why the consumer believes an error exists and include to the extent possible the type, date, and amount of the error. 12 C.F.R. § 1005.11(b)(1). Consumers submitted Notices about Zelle transfers to Defendant Banks that satisfied these requirements. Each Defendant Bank has received hundreds of thousands of such Notices.

A. Defendant Banks Have Each Failed to Reasonably Investigate Notices of Unauthorized Transfers by Failing to Review Available and Relevant Information

281. Each Defendant Bank has failed to reasonably investigate Notices of Unauthorized Transfers by failing to review any relevant records available through EWS and other participating financial institutions.

282. When investigating such Notices, each Defendant Bank has reviewed only records in its respective possession and not the other relevant information held by EWS—or the other participating financial institutions—all of whom have agreed to participate in the network.

283. **Bank of America:** [redacted]

[redacted]

284. **Chase:** [redacted]

285. **Wells Fargo:** [redacted]

B. Bank of America and Chase Each Failed to Investigate and Treat Certain Transfers Based on Flaws in the Zelle Network as Incorrect Transfers and Errors

286. Due to inaccurate or outdated information in the Zelle Network Directory, consumers' EFTs were misdirected to unintended recipients, even though the consumer provided the correct identifying token information for the recipient, i.e., the recipient's current and accurate phone number or email address.

287. [redacted]

288. [redacted]

289. These misdirected transfers are incorrect EFTs and therefore errors under Regulation E because the funds were not transferred to the correct account.

290. **Chase:** Between 2017 and 2018, when provided with a token-directory error Notice, Chase did not categorize or investigate these Notices as potential incorrect EFTs under the bank's error-resolution procedures, [redacted]

291. In total, more than 40,000 Chase customers complained that their Zelle transfers were misdirected due to token-directory errors.

292. Of those, between January 2019 and January 2021, Chase's representatives incorrectly denied claims from 17,000 accountholders related to misdirected transfers and thus failed to provide consumers with credits for the token-directory errors.

293. [redacted]

294. [redacted]

295. **Bank of America**: Between 2017 and late 2018, when provided with a token-directory error Notice, Bank of America did not categorize or investigate these Notices as potential incorrect EFTs under the bank's error-resolution procedures, [redacted]

[redacted]

296. Instead, Bank of America denied consumers' Notices on the ground that the transfers had been voluntarily sent. Up to 15,000 transfers from consumers with Bank of America accounts were misdirected due to errors in the Zelle Network Directory.

C. Defendant Banks Have Each Failed to Investigate and Treat Certain Transfers Based on Fraud or Theft as Unauthorized Transfers and Errors

297. When receiving a Notice in which a consumer alleged that a transfer from their account was initiated by a person who obtained the consumer's access device through fraud or theft and for which the consumer received no benefit, Defendant Banks have failed to investigate such Notices and treat those transfers as Unauthorized Transfers, and thus errors, in violation of EFTA and Regulation E.

a. Account Takeovers Based on Fraud

298. When Defendant Banks' customers submitted Notices asserting that they were fraudulently induced to provide their one-time passcode to a fraudster, the fraudster then accessed the consumer's device to send transfers without authorization, and the consumers received no benefit from such transfers ("Fraud Transfers"), Defendant Banks often have failed to reasonably investigate such Notices and treat such fraudulent transfers as Unauthorized Transfers and errors under EFTA and Regulation E. Instead, they have deemed such fraudulent transfers as authorized and denied the consumers' claims.

299. **Bank of America**: [redacted]

300. As a result, Bank of America failed to reasonably investigate Notices or limit consumers' liability for Fraud Transfers. [redacted]

301. **Chase**: From September 2017 to at least October 2021, when Chase customers submitted Notices about Fraud Transfers, Chase deemed such transfers as authorized and denied the consumers' claims after little to no investigation.

302. [redacted]

303. [redacted]

304. **Wells Fargo**: When Wells Fargo customers have submitted Notices about Fraud Transfers, in certain instances, Wells Fargo has failed to reasonably investigate such Notices and treat such Fraud Transfers as Unauthorized Transfers and errors under EFTA and Regulation E.

305. [redacted]

b. Account Takeovers Based on Theft

306. When Defendant Banks' customers submitted Notices asserting that their access devices, such as phones or laptops, had been stolen, the thieves made transfers from the stolen device, and the consumers received no benefit from such transfers, Defendant Banks often have failed to reasonably investigate such Notices and treat such transfers as Unauthorized Transfers and errors under EFTA and Regulation E. Instead, they have deemed such transfers as authorized and denied the consumers' claims.

307. **Bank of America:** When Bank of America customers submitted Notices asserting that their phones or laptops had been stolen and transfers were sent without their authorizations or to their benefit, Bank of America denied certain of these claims based, in part, on its determinations that previous transfers had been sent from the device, even though such determinations have no bearing on whether the device had since been stolen.

308. [redacted]

309. **Chase:** When Chase customers submitted Notices asserting that their phones or laptops had been stolen and transfers were sent without consumers' authorizations or to their benefit, Chase has denied the claims based, in part, on its determinations that no new device had been added to the customers' account and that previous transfers had been sent from the device, even though such determinations have no bearing on whether the device had since been stolen.

310. [redacted]

[redacted]

311. **Wells Fargo:** When Wells Fargo customers submitted Notices asserting that their phones had been stolen and transfers were sent without consumers' authorizations or to their benefit, Wells Fargo has repeatedly denied the claims based, in part or in whole, on non-dispositive information, such as its determinations about the device's history, password changes, and login failures, even though such determinations have no bearing on whether the device had since been stolen.

312. [redacted]

a. [redacted]

b. [redacted]

c. [redacted]

313. [redacted]

[redacted]

[redacted]

CAUSES OF ACTION
Violations of the Consumer Financial Protection Act

314. Sections 1031 and 1036 of the CFPA prohibit a "covered person or service provider" from committing or engaging in any "unfair, deceptive, or abusive act or practice" in connection with "any transaction with a consumer for a consumer financial product or service, or the offering of a consumer financial product or service." 12 U.S.C. §§ 5531(a), 5536(a)(1)(B).

315. The CFPA defines an unfair act or practice as one that (1) "causes or is likely to cause substantial injury to consumers," (2) "which is not reasonably avoidable by consumers," and (3) which "is not outweighed by countervailing benefits to consumers or to competition." 12 U.S.C. § 5531(c).

COUNT 1—CFPA
EWS has acted unfairly by failing to take timely, appropriate, and effective measures to prevent, detect, limit, and address fraud on the Zelle network.

316. The allegations in paragraphs 1-18, 22, and 24-272 are incorporated by reference.

317. EWS has engaged in unfair acts or practices by failing to take timely, appropriate, and effective network-wide measures to prevent, detect, limit, and address Zelle fraud.

318. EWS, as the network operator, has, among other failures, failed to have timely, effective, and appropriate measures for:

a. authenticating, verifying, and registering Zelle users, the absence of which has permitted bad actors to operate on the Zelle network to perpetuate fraud;

b. providing information to consumers about the identity of recipients, which has it made easier for bad actors to commit fraud;

c. providing certain risk-related information to—and, when available, requiring its use by—participating financial institutions when pausing or blocking suspicious or risky transfers;

d. suspending or restricting bad actors from using Zelle;

e. requiring participating financial institutions to report timely and accurate information about fraud; and

f. monitoring and enforcing the network rules.

319. These failures caused or were likely to cause substantial injuries to consumers, including funds lost to fraudulent transfers that EWS failed to prevent, detect, limit, or address.

320. Consumers could not reasonably avoid these injuries because of (1) consumers' lack of control over EWS's network-wide fraud prevention failures set forth in Paragraph 318; (2) EWS's representations around the safety and security of using Zelle and its insufficient warnings about Zelle fraud; and (3) the irrevocability of a Zelle transfer and the lack of adequate recourse after a transfer was made.

321. This substantial injury was not outweighed by countervailing benefits to consumers or to competition. Lack of sufficient fraud protection does not benefit consumers or competition.

322. EWS therefore has engaged in unfair acts or practices in violation of the CFPA. 12 U.S.C. §§ 5531(a), 5536(a)(1)(B).

COUNT 2—CFPA
Bank of America has acted unfairly by failing to take timely, appropriate, and effective measures to prevent, detect, limit, and address fraud on the Zelle network.

323. The allegations in paragraphs 1-17, 19, and 22-179 are incorporated by reference.

324. Bank of America has engaged in unfair acts or practices by failing to take timely, appropriate, and effective measures to prevent, detect, limit, and address Zelle fraud.

325. Bank of America has, among other failures, failed to have timely, effective, and appropriate measures for:

a. authenticating, verifying, and registering Zelle users, the absence of which has permitted bad actors to operate on the Zelle network to perpetuate fraud;

b. providing information to consumers about the identity of recipients, which has it made easier for bad actors to commit fraud;

c. pausing or blocking suspicious or risky transfers;

d. suspending or restricting bad actors from using Zelle;

e. timely reporting, or reporting at all, consumer claim information about fraudulent activity; and

f. using relevant information about fraud in consumer complaints to prevent future fraud.

326. These failures caused or were likely to cause substantial injury to consumers, including funds lost to fraudulent transfers that Bank of America failed to prevent, detect, limit, or address.

327. Consumers could not reasonably avoid these injuries because of (1) consumers' lack of control over Bank of America's fraud prevention failures set forth in Paragraph

324; (2) consumers' lack of control over Bank of America's failure to comply with certain of the network rules; (3) Bank of America's representations around the safety and security of using Zelle and its insufficient warnings about Zelle fraud; and (4) the irrevocability of the transfer and the lack of adequate recourse after a transfer was made.

328. This substantial injury was not outweighed by countervailing benefits to consumers or to competition. Lack of sufficient fraud protection does not benefit consumers or competition.

329. Bank of America therefore has engaged in unfair acts or practices, in violation of the CFPA. 12 U.S.C. §§ 5531(a), 5536(a)(1)(B).

COUNT 3—CFPA
Chase has acted unfairly by failing to take timely, appropriate, and effective measures to prevent, detect, limit, and address fraud on the Zelle network.

330. The allegations in paragraphs 1-17, 20, 22-117, and 180-230 are incorporated by reference.

331. Chase has engaged in unfair acts or practices by failing to take timely, appropriate, and effective measures to prevent, detect, limit, and address Zelle fraud.

332. Chase has, among other failures, failed to have timely, effective, and appropriate measures for:

a. authenticating, verifying, and registering Zelle users, the absence of which has permitted bad actors to operate on the Zelle network to perpetuate fraud;

b. providing information to consumers about the identity of recipients, which has it made easier for bad actors to commit fraud;

c. pausing or blocking suspicious or risky transfers;

d. suspending or restricting bad actors from using Zelle;

e. timely reporting, or reporting at all, consumer claim information about fraudulent activity; and

f. using relevant information about fraud in consumer complaints to prevent future fraud.

333. These failures caused or were likely to cause substantial injury to consumers, including funds lost to fraudulent transfers that Chase failed to prevent, detect, limit, or address.

334. Consumers could not reasonably avoid these injuries because of (1) consumers' lack of control over Chase's fraud prevention failures set forth in Paragraph 332; (2) consumers' lack of control over Chase's failure to comply with certain of the network rules; (3) Chase's representations around the safety and security of using Zelle and its insufficient warnings about Zelle fraud; and (4) the irrevocability of the transfer and the lack of adequate recourse after a transfer was made.

335. This substantial injury was not outweighed by countervailing benefits to consumers or to competition. Lack of sufficient fraud protection does not benefit consumers or competition.

336. Chase therefore has engaged in unfair acts or practices, in violation of the CFPA. 12 U.S.C. §§ 5531(a), 5536(a)(1)(B).

COUNT 4—CFPA
Wells Fargo has acted unfairly by failing to take timely, appropriate, and effective measures to prevent, detect, limit, and address fraud on the Zelle network.

337. The allegations in paragraphs 1-17, 21-117, and 231-272 are incorporated by reference.

338. Wells Fargo has engaged in unfair acts or practices by failing to take timely, appropriate, and effective measures to prevent, detect, limit, and address Zelle fraud.

339. Wells Fargo has, among other failures, failed to have timely, effective, and appropriate measures for:

a. authenticating, verifying, and registering Zelle users, the absence of which has permitted bad actors to operate on the Zelle network to perpetuate fraud;

b. providing information to consumers about the identity of recipients, which has it made easier for bad actors to commit fraud;

c. pausing or blocking suspicious or risky transfers;

d. suspending or restricting bad actors from using Zelle;

e. timely reporting, or reporting at all, consumer claim information about fraudulent activity; and

f. using relevant information about fraud in consumer complaints to prevent future fraud.

340. These failures caused or were likely to cause substantial injury to consumers, including funds lost to fraudulent transfers that Wells Fargo failed to prevent, detect, limit, or address.

341. Consumers could not reasonably avoid these injuries because of (1) consumers' lack of control over Wells Fargo's fraud prevention failures set forth in Paragraph 339; (2) consumers' lack of control over Wells Fargo's failure to comply with certain of the network rules; (3) Wells Fargo's representations around the safety and security of using Zelle and its insufficient warnings about Zelle fraud; and (4) the irrevocability of the transfer and the lack of adequate recourse after a transfer was made.

342. The substantial injury was not outweighed by countervailing benefits to consumers or to competition. Lack of sufficient fraud protection does not benefit consumers or competition.

343. Wells Fargo therefore has engaged in unfair acts or practices, in violation of the CFPA. 12 U.S.C. §§ 5531(a), 5536(a)(1)(B).

Violations of the Electronic Funds Transfer Act

344. EFTA, 15 U.S.C. § 1693 et seq., and its implementing regulation, Regulation E, 12 C.F.R. pt. 1001, establish the rights, liabilities, and responsibilities of participants in electronic fund transfer systems.

COUNT 5—EFTA and Regulation E
Bank of America has failed to follow the error-resolution requirements of EFTA and Regulation E by not treating certain transfers as incorrect and unauthorized EFTs and failing to reasonably investigate Notices of Error.

345. The allegations in paragraphs 273-283, 286-289, 295-300, and 306-308 are incorporated by reference.

346. If a financial institution receives a Notice, the institution must comply with the error resolution provisions of Regulation E, which include investigating, determining

whether an error occurred, and correcting the error if appropriate. 15 U.S.C. § 1693f(a), (b); 12 C.F.R. §§ 1005.6, 1005.11(c).

347. Bank of America, upon receipt of Notices of unauthorized and incorrect Zelle transfers:

a. has failed to reasonably investigate such Notices by not considering relevant information held by EWS or other participating financial institutions and by relying on incomplete and non-dispositive information;

b. failed to reasonably investigate Notices concerning token-directory errors or to determine that such misdirected transfers are errors under Regulation E and EFTA; and

c. failed to reasonably investigate Notices concerning unauthorized transfers executed by third parties who had fraudulently induced consumers into providing account access or had obtained account access through theft or to determine that such transfers are errors under Regulation E and EFTA.

348. As a result, Bank of America has violated the error resolution and unauthorized transfer liability provisions under EFTA, 15 U.S.C. § 1693f, and Regulation E, 12 C.F.R. §§ 1005.6, 1005.11(c).

COUNT 6—EFTA and Regulation E
Chase has failed to follow the error-resolution requirements of EFTA and Regulation E by not treating certain transfers as incorrect and unauthorized EFTs and failing to reasonably investigate Notices of Error.

349. The allegations in paragraphs 273-282, 284, 286-294, 297-298, 301-303, 306, and 309-310 are incorporated by reference.

350. If a financial institution receives a Notice, the institution must comply with the error resolution provisions of Regulation E, which include investigating, determining whether an error occurred, and correcting the error if appropriate. 15 U.S.C. § 1693f(a), (b); 12 C.F.R. §§ 1005.6, 1005.11(c).

351. Chase, upon receipt of Notices of unauthorized and incorrect Zelle transfers:

a. has failed to reasonably investigate such Notices by not considering relevant information held by EWS or other participating financial institutions and by relying on incomplete and non-dispositive information;

b. failed to reasonably investigate Notices concerning token-directory errors or to determine that such misdirected transfers are errors under Regulation E and EFTA; and

c. has failed to reasonably investigate Notices concerning unauthorized transfers executed by third parties who had fraudulently induced consumers into providing account access or had obtained account access through theft or to determine that such transfers are errors under Regulation E and EFTA.

352. As a result, Chase has violated the error resolution and unauthorized transfer liability provisions under EFTA, 15 U.S.C. § 1693f, and Regulation E, 12 C.F.R. §§ 1005.6, 1005.11(c).

COUNT 7—EFTA and Regulation E
Wells Fargo has failed to follow the error-resolution requirements of EFTA and Regulation E by not treating certain transfers as incorrect and unauthorized EFTs and failing to reasonably investigate Notices of Error.

353. The allegations in paragraphs 273-282, 285, 297-298, 304-306, and 311-313 are incorporated by reference.

354. If a financial institution receives a Notice, the institution must comply with the error resolution provisions of Regulation E, which include investigating, determining whether an error occurred, and correcting the error if appropriate. 15 U.S.C. § 1693f(a)-(b); 12 C.F.R. §§ 1005.6, 1005.11(c).

355. Wells Fargo, upon receipt of Notices of unauthorized Zelle transfers:

a. has failed to reasonably investigate such Notices by not considering relevant information held by EWS or other participating financial institutions and by relying on incomplete and non-dispositive information; and

b. has failed to reasonably investigate Notices concerning unauthorized transfers executed by third parties who had fraudulently induced consumers into providing account access or had obtained account access through theft or to determine that such transfers are errors under Regulation E and EFTA.

356. As a result, Wells Fargo has violated the error resolution and unauthorized transfer liability provisions under EFTA, 15 U.S.C. § 1693f, and Regulation E, 12 C.F.R. §§ 1005.6, 1005.11(c).

COUNT 8—CFPA
Violating Federal Consumer Financial Law (as to Bank of America)

357. The Bureau incorporates and re-alleges by reference Paragraphs 273-283, 298, 299-300, 306-308, and 345-348 of this Complaint.

358. The CFPA prohibits covered persons from offering or providing consumer-financial products or services not in conformity with "Federal consumer financial law" or otherwise committing any act or omission in violation of a "Federal consumer financial law." 12 U.S.C. § 5536(a)(1)(A).

359. Regulation E and EFTA are "Federal consumer financial law[s]." 12 U.S.C. § 5481(14).

360. As a result, the violations of EFTA and Regulation E committed by Bank of America described in Count 5 above, constitute violations of the CFPA. 12 U.S.C. § 5536(a)(1)(A).

COUNT 9—CFPA
Violating Federal Consumer Financial Law (as to Chase)

361. The Bureau incorporates and re-alleges by reference Paragraphs 273-282, 284, 286-294, 298-303, 306, 309-310, and 349-352 of this Complaint.

362. The CFPA prohibits covered persons from offering or providing consumer-financial products or services not in conformity with "Federal consumer financial law" or otherwise committing any act or omission in violation of a "Federal consumer financial law." 12 U.S.C. § 5536(a)(1)(A).

363. Regulation E and EFTA are "Federal consumer financial law[s]." 12 U.S.C. § 5481(14).

364. As a result, the violations of EFTA and Regulation E committed by Chase, described in Count 6 above, constitute violations of the CFPA. 12 U.S.C. § 5536(a)(1)(A).

COUNT 10—CFPA
Violating Federal Consumer Financial Law (as to Wells Fargo)

365. The Bureau incorporates and re-alleges by reference Paragraphs 273-285, 298, 304-306, 311-313, and 353-356 of this Complaint.

366. The CFPA prohibits covered persons from offering or providing consumer-financial products or services not in conformity with "Federal consumer financial law" or otherwise committing any act or omission in violation of a "Federal consumer financial law." 12 U.S.C. § 5536(a)(1)(A).

367. Regulation E and EFTA are "Federal consumer financial law[s]." 12 U.S.C. § 5481(14).

368. As a result, the violations of EFTA and Regulation E committed by Wells Fargo, described in Count 7 above, constitute violations of the CFPA. 12 U.S.C. § 5536(a)(1)(A).

DEMAND FOR RELIEF

WHEREFORE, Plaintiff respectfully requests that the Court issue an order and judgment pursuant to 12 U.S.C. § 5565(a)(2):

a. Permanently enjoining Defendants from committing future violations of the CFPA, EFTA, and Regulation E in connection with peer-to-peer payments;

b. Granting additional injunctive relief as the Court may deem just and proper;

c. Ordering monetary relief, including but not limited to the refund of monies paid; restitution; disgorgement or compensation for unjust enrichment; and the payment of damages;

d. Imposing on Defendants a civil money penalty under 12 U.S.C. § 5565(c);

e. Awarding costs against Defendants under 12 U.S.C. § 5565(b); and

f. Awarding additional relief as the Court may determine to be just and proper.

Dated: December 20, 2024

Respectfully submitted,
ERIC HALPERIN
Enforcement Director

DEBORAH MORRIS
Deputy Enforcement Director

JEAN M. HEALEY
Assistant Deputy Enforcement Director

MICHAEL FAVRETTO
Assistant Deputy Enforcement Director

/s/ Benjamin R. Brunner

Attorneys for Plaintiff,
CONSUMER FINANCIAL
PROTECTION BUREAU

Benjamin R. Brunner (IL Bar # 6312432)
Benjamin Buchholz (DC Bar # 1780676)
Benjamin J. Clark (IL Bar # 6316861)
Christina Coll (CA Bar # 250712)
Alexis Christensen (DC Bar # 1723838)
Stephen Jacques (DC Bar # 464413)
Amanda Roberson (MN Bar # 0398511)
Noah Steimel (DC Bar # 1723832)
Samuel Taxy (IL Bar # 6333449)
1700 G Street, NW
Washington, DC 20552
Benjamin.Brunner@cfpb.gov, (681) 393-4915
Benjamin.Buchholz@cfpb.gov, (202) 445-8908
Benjamin.Clark@cfpb.gov, (202) 435-7871
Christina.Coll@cfpb.gov, (202) 435-7843
Alexis.Christensen@cfpb.gov, (202) 435-7301
Stephen.Jacques@cfpb.gov, (202) 435-7368
Amanda.Roberson@cfpb.gov, (202) 435-9447
Noah.Steimel@cfpb.gov, (202) 435-7985
Samuel.Taxy@cfpb.gov, (202)-435-7551