

EXHIBIT H

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

EDELSBERG LAW, P.A.
Scott Edelsberg (CA Bar No. 330090)
scott@edelsberglaw.com
1925 Century Park East, Suite 1700
Los Angeles, CA 90067
Tel: 305-975-3320
Fax: 786-623-0915

KALIELGOLD PLLC
Jeffrey D. Kaliel (CA Bar No. 238293)
jkaliel@kalielpllc.com
1100 15th Street NW, 4th Floor
Washington, D.C. 20005
Telephone: (202) 350-4783

KALIELGOLD PLLC
Sophia G. Gold (CA Bar No. 307971)
sgold@kalielgold.com
950 Gilman Street, Suite 200
Berkeley, CA 94710
Telephone: (202) 350-4783

Attorneys for Plaintiff and the Putative Class

SUPERIOR COURT OF THE STATE OF CALIFORNIA

FOR THE COUNTY OF ORANGE

NATALIE TRISTAN, individually, and on
behalf of all others similarly situated,

Plaintiff,

v.

BANK OF AMERICA, N.A.,

Defendant.

Case No.: 30-2022-01255728-CU-FR-
CJC

**AMENDED CLASS ACTION
COMPLAINT**

JURY TRIAL DEMANDED

1 Plaintiff Natalie Tristan, individually and on behalf of all others similarly situated, hereby
2 brings this Amended Class Action Complaint against Defendant Bank of America, N.A. (“BOA,”
3 “Bank,” or “Defendant”) and alleges as follows:

4 **INTRODUCTION**

5 1. This lawsuit is brought as a class action on behalf of Plaintiff and thousands of
6 similarly situated customers of BOA who have signed up for the Zelle money transfer service
7 and who: have been the victim of fraud on the Zelle service; who have incurred losses due to that
8 fraud that have not been reimbursed by BOA; and who were entitled by the marketing
9 representations of BOA regarding the Zelle service and by the BOA’s contract promises to a full
10 reimbursement of losses caused by fraud on the Zelle service.

11 2. Zelle is a person-to-person (“P2P”) payment transfer service wholly owned and
12 operated by seven of the largest banks in the U.S. Person-to-Person payments allow a consumer
13 to send money to another person without needing to write a check, swipe a physical card, or
14 exchange cash.

15 3. There are approximately 1,500 member banks and credit unions who participate in
16 the Zelle service. Those members engage in their own significant marketing efforts to encourage
17 their accountholders to sign up for the Zelle service by marketing Zelle as a fast, safe and secure
18 way for consumers to send money. This is false. In fact, there are huge, undisclosed security risks
19 of using the service that BOA omitted from its marketing push to get its accountholders to sign
20 up for Zelle.

21 4. BOA prominently touts Zelle to its accountholders as a secure, free and convenient
22 way to make money transfers. However, it misrepresents and omits a key fact about the service
23 that is unknown to accountholders: that there is virtually no recourse for consumers to recoup
24 losses due to fraud. Indeed, unlike virtually every other payment method commonly used by
25 American consumers—debit cards, credit cards, and checks—there is a no protection for
26 accountholders who are victims of fraud, and virtually no recourse for accountholders attempting
27 to recoup losses due to fraud.

1 5. The unique, misrepresented, and undisclosed architecture of the Zelle payment
2 system means—again, unlike other payment options commonly used by American consumers—
3 that virtually any money transferred for any reason via Zelle is gone forever, without recourse,
4 reimbursement or protection.

5 6. Worse, BOA misrepresents and omits the truth about a secret policy it has adopted:
6 it does not and will not reimburse its accountholders for losses via Zelle due to fraud, even where
7 those losses are timely reported by accountholders.

8 7. BOA was required not to misrepresent the unique and dangerous features of the
9 Zelle service in its marketing about it and in contractual representations. But it failed to do so.

10 8. As a result, users like Plaintiff sign up for and use the Zelle service without the
11 benefit of accurate information regarding that service, and later end up with huge, unreimbursed
12 losses due to fraud. Such users never would have signed up for Zelle in the first place if they had
13 known the extreme risks of signing up for and using the service.

14 9. As a member of the Zelle network, the risks are well known to BOA but are omitted
15 from all of its marketing regarding Zelle.

16 10. As a recent New York Times investigation showed, fraud on the Zelle network is a
17 widespread scourge of which bank is well aware. Quoting an industry expert, the *Times* reported:

18 “Organized crime is rampant,” said John Buzzard, Javelin’s lead fraud analyst. “A
19 couple years ago, we were just starting to talk about it” on apps like Zelle and Venmo,
20 Mr. Buzzard said. “Now, it’s common and everywhere.”

21 The banks are aware of the widespread fraud on Zelle. When Mr. Faunce called [his
22 bank] to report the crime, the customer service representative told him, “A lot of people
23 are getting scammed on Zelle this way.” Getting ripped off for \$500 was “actually
24 really good,” Mr. Faunce said the rep told him, because “many people were getting hit
25 for thousands of dollars.”

26 <https://www.nytimes.com/2022/03/06/business/payments-fraud-zelle-banks.html> (last accessed
27 March 28, 2022).

1 **FACTUAL ALLEGATIONS**

2 **A. Overview**

3 18. It is free to sign up with Zelle, and in fact Zelle is integrated into the websites and
4 mobile apps of BOA. In marketing and within the website and app itself, BOA encourages its
5 accountholders to sign up for the Zelle service—a sign up that occurs quickly within the BOA
6 website or mobile app. During that sign-up process, a user provides basic information to Zelle
7 to link into the Zelle network.

8 19. While Zelle provides a link to what it calls a “User Agreement” on its website, at
9 no time during the sign-up process on the bank’s website or app did Plaintiff agree to be bound
10 by that document.

11 20. Sign up for the Zelle service allows the fast transfer of account funds to other Zelle
12 users.

13 21. Created in 2017 by the largest banks in the U.S. to enable instant digital money
14 transfers, Zelle is by far the country’s most widely used money transfer service. Last year, people
15 sent \$490 billion in immediate payment transfers through Zelle.

16 22. The Zelle network is operated by Early Warning Services, a company created and
17 owned by seven banks, including Defendant: Bank of America, Capital One, JPMorgan Chase,
18 PNC, Truist, U.S. Bank and Wells Fargo.

19 23. The Zelle service is very popular, but it also has a massive fraud problem—in no
20 small part because of the immediacy with which money transfers are made on the service. If a
21 fraudster removes money from a Zelle user’s bank account, either directly or by fooling the Zelle
22 user to transfer money, those funds are unrecoverable to the consumer.

23 24. Nearly 18 million Americans were defrauded through scams involving person-to-
24 person payment apps like Zelle in 2020 alone, according to Javelin Strategy & Research, an
25 industry consultant.

26 25. Organized crime is rampant on Zelle and other similar person-to-person transfer
27 services.

1 26. The 1500 banks and credit unions who are members of the Zelle network, including
2 BOA, know full well that they have a widespread fraud problem on their hands, but have
3 misrepresented and failed to take steps to warn their accountholders of these risks—or protect
4 their accountholders who fall prey to fraud.

5 27. For example, a common scam involves a scammer impersonating a bank employee
6 and requesting that the accountholder transfer money to a different bank account for testing
7 purposes. Unsuspecting Zelle users, tricked into making a fraudulent transfer, in many cases send
8 hundreds or thousands of dollars to fraudsters.

9 28. In another very common scheme, a Zelle user’s phone is stolen and Zelle transfers
10 are made from the stolen phone to the fraudster.

11 29. In short, and unbeknownst to average Zelle users, the Zelle network has become a
12 preferred tool for fraudsters like romance scammers, cryptocurrency con artists and those who
13 use social media sites to advertise fake concert tickets and purebred puppies.

14 30. Scams like these are rampant on the Zelle network precisely because of the design
15 and architecture of the network, specifically that money transfer is instantaneous and
16 unrecoverable. Indeed, there is virtually no recourse for consumers to recoup losses due to fraud,
17 unlike other payment methods commonly used by American consumers—debit cards, credit
18 cards, and checks. Zelle provides no protection for accountholders who are victims of fraud, and
19 BOA provides virtually no recourse for accountholders attempting to recoup losses due to fraud.

20 31. The unique, misrepresented, and undisclosed architecture of the Zelle payment
21 system and BOA’s own fraud policies means—again, unlike other payment options commonly
22 used by American consumers—that virtually any money transferred for any reason via Zelle is
23 gone forever, without recourse, reimbursement or protection for victimized accountholders.

24
25 **B. BOA Falsely Markets Zelle as a Safe and Secure Way to Transfer Money,**
26 **Omits Information Regarding the Extreme Risks of Signing Up for and**
27 **Using the Service, and Misrepresents Fraud Protections Regarding Zelle**
28 **in its Account Contract**

1 32. In its marketing about Zelle and during the Zelle signup process within the Bank’s
2 mobile app or website, the Bank makes repeated promises that Zelle is a “fast, **safe** and easy way
3 to send and receive money” (emphasis added).

4 33. It also promises: “Move money in the moment. It’s simple and **secure** – with lots
5 of people you know” (emphasis added),

6 34. At no time in its marketing or during the sign-up process does BOA warn potential
7 users of the true security risks of using the Zelle service—including the risk of fraud and the risk
8 that fraudulent losses will never be reimbursed by BOA.

9 35. Zelle’s services can cause unsuspecting consumers like Plaintiff to incur massive
10 losses on their linked bank accounts.

11 36. BOA misrepresents (and omits facts about) the true nature, benefits, and risks of
12 the Zelle service, functioning of which means that users are at extreme and undisclosed risk of
13 fraud when using Zelle. Had Plaintiff been adequately informed of these risks, she would not
14 have signed up for or used Zelle.

15 37. The Bank’s marketing representations about Zelle—including within its app and
16 website—misrepresent and never disclose these risks and material facts, instead luring
17 accountholders to sign up for and use the service with promises of ease, safety and security.

18 38. These representations—which all users view during the sign-up process—are false
19 and contain material omissions.

20 39. BOA misrepresents the true nature, benefits and risks of the service, which burden
21 users with an extreme and undisclosed risk of Zelle causing losses due to fraud. Plaintiff would
22 not have used Zelle if she had been adequately informed of the risks.

23 40. The Bank’s misrepresentations and omissions are especially pernicious because
24 BOA alone knows a crucial fact regarding Zelle transfers that occur on its accountholders’
25 accounts: as a matter of secret bank policy, fraud-induced Zelle transfers will almost never be
26 reimbursed to accountholders.

27
28

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

41. Indeed, upon information and belief, BOA maintains secret policy whereby it refuses to reimburse fraud losses incurred via Zelle, even where its accountholders timely inform BOA of the fraud.

42. It misrepresents and fails to disclose this secret policy.

43. Further, BOA’s Deposit Agreement & Disclosures applicable to consumer accounts repeatedly promises users that, if they timely report fraud, such fraud will be fairly investigated and accountholders will not be liable for fraudulent transfers:

Consumer’s Liability for Unauthorized Transfers

Tell us AT ONCE if you believe your card or your personal identification number (PIN) or other code has been lost or stolen. Also, tell us AT ONCE if you believe that an electronic fund transfer has been made without your permission using information from your check. The best way to keep your possible losses down is to call us immediately. Your losses could include all of the money in your account plus, if you have an overdraft protection plan linked to your account, any transfers from another account or any advances on a credit line.

If you tell us within two business days after you learn of the loss or theft of your card or code, you can lose no more than \$50 if someone uses your card without your permission.

If you do NOT tell us within two business days after you learn of the loss or theft of your card or code, and we can prove we could have stopped someone from using your card or code without your permission if you had told us, you could lose as much as \$500.

Also, if your statement shows transfers that you did not make, including those made by card, code or other means, tell us at once. If you do not tell us in writing within 60 days after the statement was mailed to you, you may not get back any money you lost after the 60 days if we can prove that we could have stopped someone from taking the money if you had told us in time. If a good reason (such as a long trip or hospital stay) kept you from telling us, we will extend the time periods.

Note: These liability rules are established by Regulation E, which does not apply to business deposit accounts. For personal deposit accounts, our liability policy regarding unauthorized debit card or ATM card transactions, and unauthorized Online Banking transactions may give you more protection, provided you report the transactions promptly. Please see the agreement you receive with your ATM or debit card and the Online Banking agreement.

[...]

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

Contact in Event of Unauthorized Transfer; and Lost or Stolen Card, PIN or Other Code

If you believe your card, PIN or other code is lost or stolen, or learned by an unauthorized person, or that someone has transferred or may transfer money from your account without your permission, notify us immediately by calling the number listed below.

Telephone: 1.800.432.1000

You can also write to us at: Bank of America, P.O. Box 53137, #7405, Phoenix, AZ 85072-3137

You should also call the number or write to the address listed above if you believe a transfer has been made using the information from your check without your permission.

If unauthorized activity occurs, you agree to cooperate during the investigation and to complete a Lost/Stolen Card and Fraud Claims Report or similar affidavit.

[...]

In Case of Errors or Questions about your Electronic Transfers You May Sign into Online Banking to Report the Error Promptly, or Call or write us at the telephone number or address below, as soon as you can, if you think your statement or receipt is wrong, or if you need more information about a transfer listed on the statement or receipt.

Call us at 1.800.432.100 during normal Claims Department business hours or write us at Bank of America, P.O. Box 53137, #7405, Phoenix, AZ 85072-3137.

We MUST hear from you NO LATER than 60 days after we sent you the FIRST statement on which the error or problem appeared... We will determine whether an error occurred within 10 business days after we hear from you and will correct any error promptly. If we need more time, however, we may take up to 45 days to investigate your complaint or question... For errors involving new accounts, point of sale, or foreign-initiated transfers transactions, we may take up to 90 days (instead of 45) to investigate your complaint or question... We will tell you the results within 3 business days after completing our investigation. If we decided that there was no error, we will send you a written explanation. You may ask for copies of the documents that we used in our investigation.

44. These provisions are and were reasonably understood by Plaintiff to mean that Plaintiff would not be liable for electronic funds transfers effectuated by fraud.

///
///
///

1 **C. BOA Is Required to Follow EFTA Requirements and It Fails to do So**

2 45. The Electronic Fund Transfer Act requires banks to reimburse customers for losses
3 on transfers that were “initiated by a person other than the consumer without actual authority to
4 initiate the transfer.”¹

5 46. An unauthorized Electronic Fund Transfer (“EFT”) is an EFT from a consumer’s
6 account initiated by a person other than the consumer without actual authority to initiate the
7 transfer and from which the consumer receives no benefit. 12 C.F.R. § 1005.2(m).

8 47. Unauthorized EFTs include transfers initiated by a person who obtained a
9 consumer’s access device through fraud or robbery and consumer transfers at an ATM that were
10 induced by force. Comment 2(m)-3 and 4.

11 48. According to the Consumer Financial Protection Bureau (“CFPB”), “If a consumer
12 has provided timely notice of an error under 12 CFR 1005.11(b)(1) and the financial institution
13 determines that the error was an unauthorized EFT, the liability protections in Regulation E
14 section 1005.6 would apply.”²

15 49. Recent CFPB guidance on unauthorized EFTs indicates P2P payments are EFTs,
16 such as transactions made with Zelle, and trigger “error resolution obligations” to consumers to
17 protect them from situations where they are fraudulently induced to initiate an unauthorized EFT
18 from a third-party.³

19 50. The CFPB has made it clear that a transaction that is fraudulently induced by a
20 third party is an unauthorized electronic funds transfer subject to the limitations of liability in 12
21 C.F.R. § 1005.6.⁴

22 51. Even so, Defendant has not reversed or refunded all funds of Plaintiff’s disputed
23 and unauthorized transactions, though obligated to do so.

24 _____
25 ¹ Electronic Fund Transfers FAQ, Consumer Financial Protection Bureau,
<https://www.consumerfinance.gov/compliance/compliance-resources/deposit-accounts-resources/electronic-fund-transfers/electronic-fund-transfers-faqs/#unauthorized-efi> (last accessed June 6, 2022).

26 ² *Id.*

27 ³ *Id.*

28 ⁴ <https://www.consumerfinance.gov/rules-policy/regulations/1005/2/> (“An unauthorized EFT includes a transfer initiated by a person who obtained the access device from the consumer through fraud”) (last accessed June 6, 2022).

1 52. Because banks, such as Defendant, fail to protect consumers as widespread “fraud
2 flourishes” on Zelle, Senators Elizabeth Warren, Robert Menendez and Jack Reed sent a letter to
3 the CEO of Zelle noting:

4 The Consumer Financial Protection Bureau previously clarified that
5 Regulation E of the Electronic Fund Transfer Act Protected victims of
6 fraudulent money transfers, including those who were “induced” into
7 transferring the money themselves, while the FDIC issued a report in
8 March 2022 finding that both the banks and the platform—in this case
Zelle—were held responsible for fraudulent electronic transfers through
Regulation E.

9 *See Exhibit 1*, Warren Letter to Zelle on Scams and Fraud (emphasis added).

10 53. Unfortunately, BOA regularly fails to consider fraudulently induced Zelle
11 transactions as “unauthorized EFTs,” thus depriving accountholders of their rights to be
12 reimbursed for such fraudulent transfers, even where the losses are timely reported by consumers.

13 **D. Plaintiff’s Experience**

14 54. When Plaintiff signed up for Zelle she was not informed that Zelle’s service had a
15 significant “catch” and that significant monetary losses could result from signing up for the
16 service—or that those losses almost never are reimbursed by users’ banks or credit unions.

17 55. For example, on November 11, 2022, a fraudster transferred \$2,150 from Plaintiff’s
18 personal bank accounts using the Zelle service.

19 56. Plaintiff is a young, college student who was searching for rental apartments online.

20 57. In November 2021, Plaintiff was searching for rental apartments and believed she
21 found a potential unit to lease online from a fraudster who went by the name of Orlin Aguilera.

22 58. Plaintiff was interested in the purported rental unit and began communicating with
23 the fraudster who informed Plaintiff to submit a rental application and fees to be screened for
24 approval as a tenant.

25 59. As the fraudster requested, Plaintiff transferred \$150 via Zelle for application fees.
26 Shortly thereafter, the fraudster informed Plaintiff that her application was “approved” and to
27 finalize obtaining the apartment, Plaintiff needed to also transfer via Zelle the security deposit of
28

1 \$800 and first-month's rent of \$1,200. Eager to secure the rental, Plaintiff transferred via Zelle
2 an additional \$2,000 to the fraudster.

3 60. Afterwards, Plaintiff and the fraudster coordinated a day and time for her to move-
4 in and collect the keys. However, on the purported move-in day, Plaintiff arrived at the apartment
5 but Orlin Aguilera, the fraudster, was nowhere to be found. The fraudster repeatedly called
6 Plaintiff with excuses for his tardiness and reassured Plaintiff that he would be arriving promptly
7 with the keys, but he never showed.

8 61. At this point, Plaintiff determined she fell victim to fraud and demanded her money
9 be returned. Despite Plaintiff's demand, the fraudster did not return the money and ceased all
10 communications with Plaintiff.

11 62. Plaintiff timely informed BOA of the fraud, but BOA refused to reimburse her for
12 the losses.

13 63. Specifically, Plaintiff immediately notified BOA once she realized the fraud.
14 Initially, BOA informed Plaintiff that she would be protected from the fraud and should expect a
15 full reimbursement of the funds. Ultimately, however, BOA denied the claim and refused to
16 reimburse Plaintiff her loss.

17 **CLASS ALLEGATIONS**

18 64. Plaintiff brings this action individually and as representatives of all those similarly
19 situated, on behalf of the below-defined Classes:

20
21 All persons with a BOA account who signed up for the Zelle Service
22 and incurred unreimbursed losses due to fraud (the "Class").

23 All California persons with a BOA account who signed up for the Zelle
24 Service and incurred unreimbursed losses due to fraud (the "California
25 Subclass").

26 65. Excluded from the Classes are Defendant and its affiliates, parents, subsidiaries,
27 employees, officers, agents, and directors. Also excluded are any judicial officers presiding over
28 this matter and the members of their immediate families and judicial staffs.

1 66. This case is appropriate for class treatment because Plaintiff can prove the elements
2 of their claims on a class wide basis using the same evidence as would be used to prove those
3 elements in individual actions alleging the same claims.

4 67. **Numerosity:** The members of the Classes are so numerous that joinder of all
5 members would be unfeasible and impracticable. The precise membership of the Classes is
6 unknown to Plaintiff at this time; however, it is estimated that the Classes are greater than one
7 hundred individuals. The identity of such membership is readily ascertainable via inspection of
8 Defendant's books and records or other approved methods. Class members may be notified of
9 the pendency of this action by mail, email, internet postings, and/or publication.

10 68. **Common Questions of Law or Fact:** There are common questions of law and fact
11 as to Plaintiff and all other similarly situated persons, which predominate over questions affecting
12 only individual Class members, including, without limitation:

- 13 a) Whether Defendant's representations and omissions about the Zelle service are
14 false, misleading, deceptive, or likely to deceive;
- 15 b) Whether Defendant failed to disclose the risks of using the Zelle service;
- 16 c) Whether Plaintiff and the Class members were damaged by Defendant's conduct;
- 17 d) Whether Defendant's actions or inactions violated the consumer protection statute
18 invoked herein;
- 19 e) Whether Defendant's actions or inactions violated the EFTA; and
- 20 f) Whether Plaintiff is entitled to a preliminary and permanent injunction enjoining
21 Defendant's conduct.

22 69. **Predominance of Common Questions:** Common questions of law and fact
23 predominate over questions that affect only individual members of the Classes. The common
24 questions of law set forth above are numerous and substantial and stem from Defendant's uniform
25 practices applicable to each individual Class member. As such, these common questions
26 predominate over individual questions concerning each Class member's showing as to his or her
27 eligibility for recovery or as to the amount of his or her damages.

1 70. **Typicality:** Plaintiff’s claims are typical of the claims of the other members of the
2 Classes because, among other things, Plaintiff and all Class members were similarly injured
3 through Defendant’s uniform misconduct as alleged above. As alleged herein, Plaintiff, like the
4 members of the Classes, were deprived of monies that rightfully belonged to them. Further, there
5 are no defenses available to Defendant that are unique to Plaintiff.

6 71. **Adequacy of Representation:** Plaintiff is an adequate class representative because
7 they are fully prepared to take all necessary steps to represent fairly and adequately the interests
8 of the members of the Classes, and because their interests do not conflict with the interests of the
9 other Class members they seek to represent. Moreover, Plaintiff’s attorneys are ready, willing,
10 and able to fully and adequately represent Plaintiff and the members of the Classes. Plaintiff’s
11 attorneys are experienced in complex class action litigation, and they will prosecute this action
12 vigorously.

13 72. **Superiority:** The nature of this action and the claims available to Plaintiff and
14 members of the Classes make the class action format a particularly efficient and appropriate
15 procedure to redress the violations alleged herein. If each Class member were required to file an
16 individual lawsuit, Defendant would necessarily gain an unconscionable advantage since it would
17 be able to exploit and overwhelm the limited resources of each individual Plaintiff with its vastly
18 superior financial and legal resources. Moreover, the prosecution of separate actions by
19 individual Class members, even if possible, would create a substantial risk of inconsistent or
20 varying verdicts or adjudications with respect to the individual Class members against Defendant,
21 and which would establish potentially incompatible standards of conduct for Defendant and/or
22 legal determinations with respect to individual Class members which would, as a practical matter,
23 be dispositive of the interests of the other Class members not parties to adjudications or which
24 would substantially impair or impede the ability of the Class members to protect their interests.
25
26
27
28

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

Further, the claims of the individual members of the Classes are not sufficiently large to warrant vigorous individual prosecution considering all of the concomitant costs and expenses attending thereto.

FIRST CAUSE OF ACTION
Violation of California’s Unfair Competition Law (“UCL”)
Cal. Bus. & Prof. Code § 17200, *et seq.*
(Asserted on Behalf of the Classes)

59. Plaintiff repeats and realleges the above allegations as if fully set forth herein.

60. California Business & Professions Code § 17200 prohibits acts of “unfair competition,” including any “unlawful, unfair or fraudulent business act or practice.”

61. Defendant’s deceptive conduct related to material omissions and/or material misrepresentations that it provides safe and secure Zelle money transfer service through its website and mobile app violates each of the statute’s “unfair,” “unlawful,” and “fraudulent” prongs.

62. The UCL imposes strict liability. Plaintiff need not prove that Defendant intentionally or negligently engaged in unlawful, unfair, or fraudulent business practices—but only that such practices occurred.

63. A business act or practice is “unfair” under the UCL if it offends an established public policy or is immoral, unethical, oppressive, unscrupulous, or substantially injurious to consumers, and that unfairness is determined by weighing the reasons, justifications, and motives of the practice against the gravity of the harm to the alleged victims.

64. Defendant’s practices as described herein are (a) immoral, unethical, oppressive, and/or unscrupulous and violate established public policy as recognized by, *inter alia*, causing injury to consumers which outweigh any purported benefits or utility.

65. A business act or practice is “fraudulent” under the UCL if it is likely to deceive members of the public.

1 66. Defendant’s practices, as described herein, constitute “fraudulent” business
2 practices in violation of the UCL because, among other things, they are likely to deceive
3 reasonable consumers, who expect their bank to fully investigate and protect fraudulent losses
4 incurred using the Zelle service. Moreover, Defendant concealed the security risks of using the
5 Zelle service, including the risk of fraud and the risk that fraudulent losses will never be
6 reimbursed by BOA as a matter of secret policy, is a practice that is likely to deceive a consumer
7 acting reasonably under the circumstances, to the consumer’s detriment.

8 67. A business act or practice is “unlawful” under the UCL if it violates any other law
9 or regulation.

10 68. Among other statutes, laws, and/or regulations, Defendant’s acts and practices
11 violate the following statutes, laws, and/or regulations:

- 12 a. Violating Cal. Civ. Code § 1750, *et seq.*;
- 13 b. Violating the EFTA;
- 14 c. Engaging in conduct in which the gravity of harm to Plaintiff and the Class
15 outweighs the utility of the Defendant’s conduct;
- 16 d. Engaging in acts and/or practices and/or omissions that are immoral, unethical,
17 oppressive, and/or unscrupulous and causes injury to consumers which outweigh
18 its benefits; and/or
- 19 e. Defendant committed unfair and fraudulent business acts and practices in violation
20 of Cal. Bus. & Prof. Code § 17200, *et seq.*, by affirmatively and knowingly
21 misrepresenting on its website and mobile app the true risks and operation of its
22 service.

23 69. Defendant’s acts and practices offend an established public policy of secure
24 electronic money transfers in the marketplace, and constitute immoral, unethical, oppressive, and
25 unscrupulous activities that are substantially injurious to consumers.

1 statement...which is untrue or misleading and which is known, or which by the exercise of
2 reasonable care should be known, to be untrue or misleading....”

3 78. Defendant’s material misrepresentations and omissions alleged herein violate Bus.
4 & Prof. Code § 17500.

5 79. Defendant knew or should have known that its misrepresentations and omissions
6 were false, deceptive, and misleading.

7 80. Pursuant to Business & Professions Code §§ 17203 and 17500, Plaintiff and the
8 members of the Classes, on behalf of the general public, seeks an order of this Court enjoining
9 Defendant from continuing to engage, use, or employ their practice of misrepresenting the Zelle
10 service.

11 81. Further, Plaintiff and the members of the Class seek an order requiring Defendant
12 to disclose such misrepresentations, and additionally request an order awarding Plaintiff
13 restitution of the money wrongfully acquired by Defendant by means of said misrepresentations.

14 82. Additionally, Plaintiff and the Class members seek an order requiring Defendant to
15 pay attorneys’ fees pursuant to Cal. Civ. Code § 1021.5.

16 **THIRD CAUSE OF ACTION**
17 **Breach of Contract Including Breach of the Covenant of Good Faith and Fair Dealing**
18 **(Asserted on Behalf of the Classes)**

19 83. Plaintiff repeats and realleges the above allegations as if fully set forth herein.

20 84. Plaintiff and members of the Classes contracted with BOA for checking account
21 services, as embodied in the Deposit Agreement & Disclosures.

22 85. BOA breached the terms of its contract with consumers when as described herein,
23 BOA failed to fairly investigate reported fraudulent transactions on the Zelle money transfer
24 service and failed to reimburse accountholders for fraud-induced losses incurred using the Zelle
25 service.

26 ///

27 ///

1 86. Further, under the law of each of the states where BOA does business, an implied
2 covenant of good faith and fair dealing governs every contract. The covenant of good faith and
3 fair dealing constrains Defendant’s discretion to abuse self-granted contractual powers.

4 87. This good faith requirement extends to the manner in which a party employs
5 discretion conferred by a contract.

6 88. Good faith and fair dealing, in connection with executing contracts and discharging
7 performance and other duties according to their terms, means preserving the spirit—not merely
8 the letter—of the bargain. Put differently, the parties to a contract are mutually obligated to
9 comply with the substance of their contract in addition to its form. Evading the spirit of the
10 bargain and abusing the power to specify terms constitute examples of bad faith in the
11 performance of contracts.

12 89. Subterfuge and evasion violate the obligation of good faith in performance even
13 when an actor believes his conduct to be justified. A lack of good faith may be overt or may
14 consist of inaction, and fair dealing may require more than honesty. Other examples of violations
15 of good faith and fair dealing are willful rendering of imperfect performance, abuse of a power
16 to specify terms, and interference with or failure to cooperate in the other party’s performance.

17 90. Defendant breached the covenant of good faith and fair dealing when it failed to
18 fairly investigate reported fraudulent transactions on the Zelle money transfer service and failed
19 to reimburse accountholders for fraud-induced losses incurred using the Zelle service.

20 91. Each of Defendant’s actions was done in bad faith and was arbitrary and capricious.

21 92. Plaintiff and members of the Classes have performed all of the obligations imposed
22 on them under the contract.

23 93. Plaintiff and members of the Classes have sustained monetary damages as a result
24 of BOA’s breaches of the contract and covenant of good faith and fair dealing.

25 ///

26 ///

27 ///

28

FOURTH CAUSE OF ACTION
Violation of the Electronic Funds Transfer Act (“EFTA”)
15 U.S.C. §§ 1693, et seq.
(Asserted on Behalf of the Classes)

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

94. Plaintiff repeats and realleges the above allegations as if fully set forth herein.

95. The Electronic Fund Transfer Act and Regulation E apply to electronic fund transfers that authorize a financial institution to debit or credit a consumer’s account. 12 C.F.R. § 1005.3(a).

96. The primary objective of the EFTA is “the protection of individual consumers engaging in electronic fund transfers and remittance transfers.” 12 C.F.R. § 1005.1(b).

97. Defendant is a financial institution. 12 C.F.R. § 1005.2(i).

98. Zelle is a financial institution, as the applicable code, 12 C.F.R. § 1005.2(i), interpreted by the Consumer Financial Protection Bureau.⁵

99. “If a financial institution, within sixty days after having transmitted to a consumer pursuant to [15 U.S.C. § 1693d(a), (c), or (d)] or notification pursuant to [15 U.S.C. § 1693d(d)] receives oral or written notice in which the consumer[:] (1) sets forth or otherwise enables the financial institution to identify the name and the account number of the consumer; (2) indicates the consumer’s belief that the documentation, or, in the case of notification pursuant to [15 U.S.C. § 1693d(b)], the consumer’s account, contains an error and the amount of such error; and (3) sets forth the reasons for the consumer’s belief (where applicable) that an error has occurred,” the financial institution is required to investigate the alleged error. 15 U.S.C. § 1693f(a).

100. After said investigation, the financial institution must determine whether an “error” has occurred and report or mail the results of such investigation and determination to the consumer within ten (10) business days. 15 U.S.C. § 1693f(a).

///

///

⁵ Electronic Fund Transfers FAQs, Consumer Financial Protection Bureau, <https://www.consumerfinance.gov/compliance/compliance-resources/deposit-accounts-resources/electronic-fund-transfers/electronic-fund-transfers-faqs/#financial-institutions-2> (last accessed June 6, 2022).

1 101. A financial institution that provisionally recredits the consumer’s account for the
2 amount alleged to be in error pending an investigation, however, is afforded forty-five (45)
3 business days after receipt of notice of error to investigate. *Id.* § 16993f(c).

4 102. Pursuant to the EFTA, an error includes “an unauthorized electronic fund transfer.”
5 *Id.* § 1693f(f).

6 103. An Electronic Fund Transfer (“EFT”) is any transfer of funds that is initiated
7 through an electronic terminal, telephone, computer, or magnetic tape for the purpose of ordering,
8 instructing, or authorizing a financial institution to debit or credit a consumer’s account. 12
9 C.F.R. 1005.3(b)(1). Accordingly, Regulation E applies to any person-to-person (“P2P”) or
10 mobile payment transactions that meet the definition of EFT. 12 C.F.R. § 1005.3(b)(1)(v); *id.*,
11 Comment 3(b)(1)-1.ii.

12 104. Unauthorized EFTs are EFTs from a consumer’s account initiated by a person other
13 than the consumer without actual authority to initiate the transfer and from which the consumer
14 receives no benefit. 12 C.F.R. § 1005.2(m).

15 105. According to the Consumer Financial Protection Bureau, when a third party
16 fraudulently induces a consumer into sharing account access information that is used to initiate
17 an EFT from the consumer’s account, that transfer meets Regulation E’s definition of an
18 unauthorized EFT.⁶

19 106. In particular, Comment 1005.2(m)-3 of Regulation E explains that an unauthorized
20 EFT includes a transfer initiated by a person who obtained the access device from the consumer
21 through robbery or fraud. As such, when a consumer is fraudulently induced into sharing account
22 access information with a third party, and a third party uses that information to make an EFT
23 from the consumer’s account, the transfer is an unauthorized EFT under regulation E. 12 C.F.R.
24 § 1005.2(m), Comment 1005.2(m)-3.

25 ///

26 _____
27 ⁶ “Electronic Fund Transfers FAQs,” Consumer Financial Protection Bureau,
28 <https://www.consumerfinance.gov/compliance/compliance-resources/deposit-accounts-resources/electronic-fund-transfers/electronic-fund-transfers-faqs/#financial-institutions-2> (last accessed June 6, 2022).

1 107. Here, Plaintiff and Members of the Classes were fraudulently induced by third-
2 party scammers to make unauthorized money transfers from their BOA accounts.

3 108. After the unauthorized EFTs were made, the EFTs appeared on the bank statements
4 of Plaintiff and Members of the Classes.

5 109. Plaintiff and Members of the Classes notified Defendant of these errors within sixty
6 (60) days of their appearances on their accounts.

7 110. As a direct and proximate result of Defendant’s conduct, Plaintiff and Members of
8 the Classes were unable to reclaim the account funds taken from scammers from unauthorized
9 EFTs.

10 111. Defendant knowingly and willfully concluded that the transfers of funds via Zelle
11 on accounts of Plaintiff and Members of the Classes were not in error when such conclusions
12 could not reasonably have been drawn from the evidence available to the financial institutions at
13 the time of the investigation. 15 U.S.C. § 1693f(e)(2).

14 112. Defendant intentionally determined that the unauthorized transfer of funds via
15 Zelle on accounts of Plaintiff and Members of the Classes were not in error due to, at least in
16 part, their financial self-interest as a stakeholder in Zelle.

17 113. Defendant refused to reverse or refund funds to Plaintiff and Members of the
18 Classes.

19 114. As such, Plaintiff and Members of the Classes are each entitled to (i) actual
20 damages; (ii) treble damages; (iii) the lesser of \$500,000.00 or one percent (1%) of the net worth
21 of Defendant; and (iv) reasonable attorneys’ fees and costs. *Id.* §§ 1693f(e)(2), 1693m(a)(2)(B)–
22 (3).

23 ///

24 ///

25 ///

26 ///

27 ///

28

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

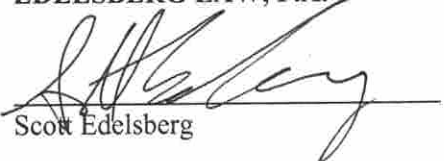
DEMAND FOR JURY TRIAL

Plaintiff and all others similarly situated hereby demand trial by jury on all issues in this Class Action Complaint that are so triable.

Dated: June 8, 2022

Respectfully submitted,

EDELSBERG LAW, P.A.



Scott Edelsberg

KALIELGOLD PLLC
Jeffrey D. Kalief
Sophia Goren Gold

Attorneys for Plaintiff and the Putative Class

EXHIBIT 1

United States Senate

WASHINGTON, DC 20510

April 29, 2022

Al Ko
Early Warning Services, LLC
16552 N 90th St
Scottsdale, AZ 85260

Dear Mr. Ko,

We write regarding disturbing reports of a rise in fraud and scams on your online peer-to-peer money transfer platform Zelle, and the ongoing failure by Zelle or the banks that own this service to address these scams and provide appropriate redress to defrauded consumers. This “widespread fraud” on money transfer apps has affected nearly 18 million Americans.¹ Given the rise of increasingly sophisticated scams on your platform and the widely documented difficulties consumers have faced in seeking relief from banks, we seek to understand the extent to which Zelle allows fraud to flourish and the steps your company is taking to increase consumer protection and help users recover lost funds.

After its introduction in 2017, Zelle exploded in popularity, in large part because its connections to large financial institutions allowed it to sell itself as “fast, free, and ubiquitous.”² Your company, Early Warning Services, LLC is owned by seven of the country’s biggest banks, including JP Morgan Chase & Co., Bank of America, and Wells Fargo, giving consumers the convenience of an integrated platform and providing an implicit promise that activity on the platform is as secure as activity at the bank teller window.³ In 2021, Zelle “drove \$490 billion in transactions, more than double Venmo’s \$230 P2P volume.”⁴

The increased activity on Zelle is putting millions of consumers at risk as fraud flourishes:

Police reports and dispatches from industry analysts make it clear that the network has become a preferred tool for grifters like romance scammers, cryptocurrency con artists, and those who prowl social media sites advertising concert tickets and purebred puppies — only to disappear with buyers’ cash after they pay.⁵

¹ New York Times, “Fraud Is Flourishing on Zelle. The Banks Say It’s Not Their Problem,” Stacy Cowley and Lananh Nguyen, March 6, 2022, <https://www.nytimes.com/2022/03/06/business/payments-fraud-zelle-banks.html>.

² New York Times, “Cash Faces a New Challenger in Zelle, a Mobile Banking Service,” Stacy Cowley, June 12, 2017, <https://www.nytimes.com/2017/06/12/business/dealbook/mobile-banking-zelle-venmo-apple-pay.html>.

³ Early Warning Services, LLC, website accessed April 25, 2022, <https://www.earlywarning.com/about>; New York Times, “Cash Faces a New Challenger in Zelle, a Mobile Banking Service,” Stacy Cowley, June 12, 2017, <https://www.nytimes.com/2017/06/12/business/dealbook/mobile-banking-zelle-venmo-apple-pay.html>.

⁴ American Banker, “Can Zelle change the narrative around P2P fraud?,” Kate Fitzgerald, March 9, 2022, <https://www.americanbanker.com/payments/news/can-zelle-change-the-narrative-around-p2p-fraud>.

⁵ New York Times, “Fraud Is Flourishing on Zelle. The Banks Say It’s Not Their Problem,” Stacy Cowley and Lananh Nguyen, March 6, 2022, <https://www.nytimes.com/2022/03/06/business/payments-fraud-zelle-banks.html>.

Reports of consumers losing thousands of dollars have come out of California,⁶ Massachusetts,⁷ and Georgia.⁸ These scams, many of which involve a scammer creating a Zelle account linked to the consumer's own phone number, have cost victims their life savings and robbed them of funds essential to their small businesses, further underscoring the consequences of this widespread fraud.⁹

Alarming, both your company and the big banks who both own and partner with the platform have abdicated responsibility for fraudulent transactions, leaving consumers with no way to get back their funds. Zelle's biggest draw – the immediacy of its transfers – also makes scams more effective and “a favorite of fraudsters,” as consumers have no option to cancel a transaction even moments after authorizing it.¹⁰ And banks have chosen to let consumers suffer, blaming them for authorizing fraudulent transactions.¹¹ According to Consumer Watchdog, banks were essentially “throw[ing] up their hands and say ‘it’s not our problem because you authenticated it.’”¹² A former executive at your company even argued that banks have not done enough to deter fraud on Zelle, warning that banks had not sufficiently educated consumers about the risks.¹³ One customer observed that “it’s like the banks have colluded with the sleazebags on the street to be able to steal.”¹⁴

The policies of your company and the banks that own and operate on it create a confusing and unfair environment for consumers, who are already facing “rampant” and sophisticated threats from spammers on the platform.¹⁵ The Consumer Financial Protection Bureau previously clarified that Regulation E of the Electronic Fund Transfer Act protected victims of fraudulent money transfers, including those who were “induced” into transferring the money themselves,¹⁶ while the FDIC issued a report in March 2022 finding that both the banks and the platform – in

⁶ ABC 7 News, “LA woman loses over \$18K through 'Zelle' after scammers text, call her pretending to be bank,” Carlos Granda, March 12, 2022, <https://abc7.com/los-angeles-zelle-scam-text-message/11644167/>.

⁷ Boston 25 News, ““They’re not robots talking to you. They’re actual people.” Zelle app users warn of latest scams,” Chris Flanagan, March 23, 2022, <https://www.boston25news.com/news/massachusetts/theyre-not-robots-talking-you-theyre-actual-people-zelle-app-users-warn-latest-scams/WJZVXE23JZFCTPBD5XOPZZXF6I/>.

⁸ WBS-TV, “Zelle warns about scams, says it’s not responsible for funds stolen through app,” Ashli Lincoln, March 28, 2022, <https://www.wsbtv.com/news/local/zelle-warns-about-scams-says-its-not-responsible-funds-stolen-through-app/ZTCNAVOTTNG5RNTAOAXPWELXB4/>.

⁹ *Id.*

¹⁰ KARE 11, “Two Minnesota women were tricked by the same scam on Zelle, here's how you can protect yourself,” Gordon Severson, March 22, 2022, <https://www.kare11.com/article/money/minnesota-women-tricked-by-the-same-scam-on-zelle-heres-how-you-can-protect-yourself/89-3016a498-c8db-407a-ab1f-632f24204d9a>; New York Times, “Fraud Is Flourishing on Zelle. The Banks Say It’s Not Their Problem,” Stacy Cowley and Lananh Nguyen, March 6, 2022, <https://www.nytimes.com/2022/03/06/business/payments-fraud-zelle-banks.html>.

¹¹ New York Times, “Fraud Is Flourishing on Zelle. The Banks Say It’s Not Their Problem,” Stacy Cowley and Lananh Nguyen, March 6, 2022, <https://www.nytimes.com/2022/03/06/business/payments-fraud-zelle-banks.html>.

¹² ABC 7, “Calif. woman loses over \$18K through 'Zelle' after scammers text, call her pretending to be bank,” Carlos Granda, March 14, 2022, <https://abc7news.com/zelle-scam-electronic-withdrawals-bank-of-america/11650620/>.

¹³ New York Times, “Fraud Is Flourishing on Zelle. The Banks Say It’s Not Their Problem,” Stacy Cowley and Lananh Nguyen, March 6, 2022, <https://www.nytimes.com/2022/03/06/business/payments-fraud-zelle-banks.html>.

¹⁴ *Id.*

¹⁵ *Id.*

this case Zelle – were held responsible for fraudulent electronic transfers through Regulation E.¹⁷ Given this regulatory landscape, your company and the banks have a clear responsibility to more aggressively protect consumers.

In order to better understand how consumers have experienced fraud on your platform we ask that you provide answers to the following questions by May 13, 2022:

1. What are the procedures for rooting out scams on the online platform Zelle, and how has your company adjusted those procedures in light of “rampant [...] organized crime”¹⁸ on the platform?
2. What are Zelle’s policies for determining which consumers receive refunds for fraudulent claims?
 - a. Is this a joint process with the account holders’ bank? If so, are these procedures standardized across all banks and financial institutions using the platform?
3. Does Regulation E of the Electronic Fund Transfers Act apply to the scams seen regularly on Zelle, including those that involve consumers induced into authorizing fraudulent transfers?
 - a. Under Regulation E, would Early Warning Services, LLC or the account holders’ bank be responsible for refunding the funds?
4. How many reports of fraud from Zelle customers have Early Warning Services received for each of the last five full calendar years, and from January 1, 2022, to the present? For each year, and for the period from January 1, 2022, to the present, please provide:
 - a. The total number of reported cases of fraud from Zelle customers.
 - b. The total dollar value of reported fraud.
 - c. The number of cases where Zelle provided refunds to customers.
 - d. The total value of these refunds.
 - e. The number of cases where Zelle referred fraud to law enforcement or to federal or state bank regulators,

Thank you for your attention to this matter.

Sincerely,

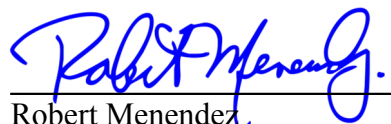
¹⁶ Boston 25 News, ““They’re not robots talking to you. They’re actual people.” Zelle app users warn of latest scams,” Chris Flanagan, March 23, 2022, <https://www.boston25news.com/news/massachusetts/theyre-not-robots-talking-you-theyre-actual-people-zelle-app-users-warn-latest-scams/WJZVXE23JZFCTPBD5XOPZZXF6I/>.

¹⁷ Consumer Finance Monitor, “FDIC Consumer Compliance Supervisory Highlights looks at unauthorized EFTs, overdraft programs, re-presentment of unpaid transactions, and fair lending,” John L. Culhane, Jr., April 7, 2022, <https://www.consumerfinancemonitor.com/2022/04/07/fdic-consumer-compliance-supervisory-highlights-looks-at-unauthorized-efts-overdraft-programs-re-presentment-of-unpaid-transactions-and-fair-lending/>.

¹⁸ New York Times, “Fraud Is Flourishing on Zelle. The Banks Say It’s Not Their Problem,” Stacy Cowley and Lananh Nguyen, March 6, 2022, <https://www.nytimes.com/2022/03/06/business/payments-fraud-zelle-banks.html>.



Elizabeth Warren
United States Senator



Robert Menendez
United States Senator



Jack Reed
United States Senator