FILED

STATE OF NORTH CAROLINA

IN THE GENERAL COURT OF JUSTICE

2022 OCT 17 P 2:

SUPERIOR COURT DIVISION

MECKLENBURG COUNTY

No. 22 CVS 16773

KANANI WOLF, individually, and on behalf of all others similarly situated, Plaintiff, v. **BANK OF AMERICA, N.A.,** Defendant.	**CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Kanani Wolf, individually and on behalf of all others similarly situated, hereby brings this Class Action Complaint against Defendant Bank of America, N.A. ("BofA," "Bank," or "Defendant") and alleges as follows:

INTRODUCTION

1. This lawsuit is brought as a class action on behalf of Plaintiff and thousands of similarly situated Bank of America accountholders who have been deceived into so-called me-to-me scams via Zelle, incurred losses, and were not reimbursed by Defendant even after being timely notified by the defrauded accountholder.

2. The Bank's misrepresentations and omissions, in marketing materials, about the Zelle money transfer service deceived its customers and damaged BofA accountholders who: have been the victim of "bank employee impersonation" fraud on the Zelle platform; who have incurred losses due to that particular fraud that have not been reimbursed by Defendant; and who were entitled by the marketing representations of Defendant regarding the Zelle service and by Defendant's contract promises to a full reimbursement of losses caused by bank employee impersonation fraud on the Zelle service.

3. Zelle is a person-to-person payment transfer service that allow a consumer to send money to another person without needing to write a check, swipe a physical card, or exchange cash.

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

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

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

7. Worse, Defendant misrepresents and omits the truth about a secret policy they have adopted: Defendant does not and will not reimburse BofA accountholders for losses via Zelle due to fraud, even where those losses are timely reported by accountholders, and even where (as with the "me-to-me" scam described below) the Bank itself provides key assistance to the scammers.

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

9. This is especially true with respect to bank employee impersonation fraud. In this common scam, also called "me-to-me" fraud, a scammer—often from a bank caller ID—tells the consumer that his or her bank account was compromised, and persuades the person to send money to what appears to be himself or herself using Zelle. In reality, the scammer has linked the consumer's cellphone to their own fraudulent Zelle account.

10. To use Zelle, customers must link either an email address or a phone number to their BofA Zelle account. If a BofA customer creates a Zelle account using only an email, then a customer's cellphone number can still be used to link to other Zelle accounts. Scammers capitalize on this inherent security flaw by linking BofA customers cellphone numbers to their own fraudulent Zelle accounts.

11. This scam cannot succeed without the assistance of the Bank, specifically the Bank's mistaken and negligent linking of a legitimate BofA accountholder's cellphone number to a scammer's Zelle account. That error is the key link that allows this scam to take place.

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

13. These risks are well known to Defendant but are omitted from all of its marketing regarding the Zelle service.

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

> "Organized crime is rampant," said John Buzzard, Javelin's lead fraud analyst. "A couple years ago, we were just starting to talk about it" on apps like Zelle and Venmo, Mr. Buzzard said. "Now, it's common and everywhere."
>
> The banks are aware of the widespread fraud on Zelle. When Mr. Faunce called [his bank] to report the crime, the customer service representative told him, "A lot of people are getting scammed on Zelle this way." Getting ripped off for $500 was "actually really good," Mr. Faunce said the rep told him, because "many people were getting hit for thousands of dollars."

Fraud Is Flourishing on Zelle. The Banks Say It's Not Their Problem, The New York Times (March 6, 2022), https://www.nytimes.com/2022/03/06/business/payments-fraud-zelle-banks.html (last accessed March 28, 2022).

15. Had Plaintiff and the Class members known of the true operation and risks of Zelle—risks Defendant alone was aware of and actively misrepresented—they would not have signed up for and used the Zelle service.

16. Plaintiff and the Class members have been injured by Defendant's practices. Plaintiff brings this action on behalf of herself, the putative Classes, and the general public. Plaintiff seeks actual damages, punitive damages, restitution, and an injunction on behalf of the general public to prevent BofA from continuing to engage in its illegal practices as described herein.

PARTIES

17. Plaintiff Kanani Wolf is a citizen and resident of Santa Monica, California.

18. Defendant Bank of America, N.A. is a federally chartered bank with its principal place of business in Charlotte, North Carolina.

JURISDICTION AND VENUE

19. This is an action for injunctive relief, violation of state consumer protection laws, and breach of contract. The amount in controversy exceeds $25,000 exclusive of interest, costs, and attorneys' fees.

20. Defendant is subject to personal jurisdiction in North Carolina as its principal place of business is in Charlotte, North Carolina.

21. Venue for this action is proper in this Court pursuant to N.C. Gen. Stat. §1-82 because Defendant Bank of America, N.A. resides in Mecklenburg County.

FACTUAL ALLEGATIONS

A. Overview

22. Created in 2017 by the largest banks in the U.S. to enable instant digital money transfers, Zelle is by far the country's most widely used money transfer service. Last year, people sent $490 billion in immediate payment transfers through Zelle.[1]

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

24. Zelle introduced itself to the American public with a massive advertising blitz starting in 2018. Zelle and partner banks marketed Zelle as a safer alternative to other instant payment apps "because it's backed by the banks."

25. Zelle's aggressive marketing touted its security features. In one TV commercial, performer Daveed Diggs from the Broadway show *Hamilton* rapped, "You can send money safely cause that's what it's for / It's backed by the banks so you know it's secure."

26. Plaintiff recalls viewing this advertisement.

27. It is free for existing BofA accountholders to sign up with Zelle, and in fact Zelle is integrated into the websites and mobile apps of BofA. In marketing and within the website and

[1] ZellePay.com, *Nearly Half a Trillion Dollars Sent by Consumers and Businesses with Zelle in 2021* (February 02, 2022), https://www.zellepay.com/press-releases/nearly-half-trillion-dollars-sent-consumers-and-businesses-zelle-2021 (last visited October 5, 2022).

app itself, Defendant encourages BofA accountholders to sign up for the Zelle service—a sign up that occurs quickly within the BofA website or mobile app.

28. During the Zelle sign-up process, users are not affirmatively provided with agreements or disclosures previously provided at the time they opened their BofA account..

29. While Zelle provides a link to what it calls a "User Agreement" on its website, at no time during the sign-up process on BofA's website or app did Plaintiff agree to be bound by that document.

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

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

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

33. Nearly 18 million people have been victims of "widespread fraud" on money transfer apps like Zelle, according to a letter sent in late April of 2022 to Zelle by U.S. Senators Elizabeth Warren of Massachusetts, Robert Menendez of New Jersey and Jack Reed of Rhode Island.[2]

[2] Letter from Elizabeth Warren, Robert Menendez, Jack Reed, Sen., U.S. Cong., to Al Ko, CEO, Early Warning Services (April 2, 2022).

34. "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," the letter stated.

35. A Senate report from October 2022 revealed that just four banks tallied 192,878 cases of fraud worth collectively $213.8 million in 2021 and the first half of 2022 where a customer claimed they had been fraudulently tricked into making a payment. In only roughly 3,500 cases did those banks reimburse the customer, the report found. Further, in the cases where it is clear funds had been taken out of customers' account without authorization, only 47% of those dollars were ever reimbursed.

36. Specifically, PNC Bank had 8,848 cases of Zelle fraud in 2020, and is on pace to have roughly 12,300 cases this year. U.S. Bank had 14,886 cases in 2020 and had 27,702 cases in 2021. Truist had 9,455 cases of fraud and scams on Zelle in 2020, which ballooned to 22,045 last year.

37. Organized crime is rampant on Zelle and other person-to-person transfer services.

38. For example, a common scam involves a scammer impersonating a bank employee who alerts the bank customer to "suspicious" or "fraudulent" account activity and offers to help prevent the alleged fraud by advising that the accountholder transfer money to a different bank account. Unsuspecting Zelle users, tricked into making a fraudulent transfer, in many cases send hundreds or thousands of dollars to fraudsters.

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

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

41. "Scams have become widespread on Zelle, a money-transfer platform owned by the largest banks in the nation," one US Senator said at an April 26 Congressional hearing. "The banks are well aware of these scams but have done little to enhance Zelle's security or reimburse defrauded consumers."

42. Craigslist, Paypal, and Venmo faced early criticism for leaving users vulnerable to fraud. In response, each made changes. Craigslist, for example, added a warning about scams on every sale listing. Paypal increased the protections it offers on some digital sales and provided a detailed disclosure about what transactions it will and won't protect.

43. And Venmo—which, like Zelle, does not protect users if a seller does not deliver what they promised—upgraded its security policies in 2015 to better detect fraud, by notifying customers when someone adds an email address or new device to their account. The Federal Trade Commission later criticized the company for not having those protections in place from the start.

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

B. Defendant Falsely Markets Zelle as a Safe and Secure Way to Transfer Money, Omits Information Regarding the Extreme Risks of Signing Up for and Using the Service, and Misrepresent Fraud Protections Regarding Zelle in its Account Contracts

45. At all relevant times, BofA's website and app featured a page devoted to explaining and marketing Zelle.

46. That page directs people immediately to the Zelle sign-up process and expressly says: "You are not liable for fraudulent Online and mobile Banking transactions when you notify the bank within 60 days of the transaction first appearing on your statement and comply with security responsibilities. See Section 5 of our Online Banking Service Agreement for full terms and conditions." Plaintiff recalls viewing this page prior to signing up.

47. Reasonable consumers like Plaintiff understand that to mean fraud is protected. BofA knows this is a reasonable assumption, especially in combination with the many "safe" representations BofA and Zelle make in their marketing. But BofA knows a secret that it does not tell consumers: it unilaterally and unreasonable decided "fraud" only means transfers initiated by someone other than the accountholder.

48. BofA has recently deleted this "fraud protection" promise.

49. In its marketing about Zelle and during the Zelle sign-up process within the Bank's mobile app or website, Defendant makes repeated promises that Zelle is a "fast, safe and easy way to send and receive money" (emphasis added).

50. Defendant also promise: "Move money in the moment. It's simple and **secure** – with lots of people you know." (emphasis added).

51. Defendant again promised: "With Zelle, money payments and requests are simple, **safe**—and free—using the Bank of America Mobile app." (emphasis added).

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

53. Defendant's Zelle service can cause unsuspecting consumers like Plaintiff to incur massive losses on their linked bank accounts.

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

55. Defendant's marketing representations about Zelle—including within BofA's app and website—misrepresent and never disclose these risks and material facts, instead luring BofA accountholders to sign up for and use the service with promises of ease, safety and security.

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

57. In its Zelle FAQs, BofA expressly stated:

1. **What is *Zelle*®?**
   The Bank of America Mobile Banking app now includes *Zelle* — the new way to send and receive money with friends, family and people you know, with a U.S. bank account, typically within minutes, no matter where they bank.

2. **Is it secure?**
   Yes, with our Bank of America Mobile Banking Security Guarantee, you are protected by the same security you're used to where you will not be liable for fraudulent transactions (when reported promptly) and we will help keep your information safe.

58. But BofA misrepresentations and omissions are especially pernicious because it alone knows a secret that it does not tell consumers: it unilaterally and unreasonable decided "fraudulent" only means transfers initiated by someone other than the accountholder.

59. Indeed, upon information and belief, the Bank maintains a secret policy whereby they refuse to reimburse fraud losses incurred via Zelle, even where its accountholders timely inform BofA of the fraud.

60. Defendant misrepresents and fails to disclose this secret policy.

61. Further, BofA's Deposit Agreement & Disclosures ("the Account 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.

62. For transactions governed by Regulation E, the Agreement states:

> **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.

[...]

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.

See Account Disclosures, at 60-61.

63. For transactions *not* governed by Regulation E, the Agreement provides:

Review Statements and Report Suspected Problems Immediately
You must promptly review the notices, statements and other communications, along with any accompanying checks and other items, we send you. You must also report problems or **unauthorized transactions** to us immediately, by calling the number for customer service on your statement.

Id., at 40 (emphasis added).

64. The Agreement further states:

What Are Problems and Unauthorized Transactions
Problems and **unauthorized transactions include suspected fraud**; missing deposits; **unauthorized electronic transfers**; missing, stolen, or unauthorized checks or other withdrawal orders; checks or other withdrawal orders bearing an unauthorized signature, endorsement or alteration; illegible images; encoding errors made by you or us; and counterfeit checks. This is not a complete list.

Id., at 42 (emphasis added).

65. The Agreement also indicates:

Except as otherwise expressly provided elsewhere in this agreement, if you fail to notify us in writing of suspected problems or **unauthorized transactions within 60 days after we make your statement or items available to you, you agree that:**
• you may not make a claim against us relating to the unreported problems or unauthorized transactions, regardless of the care or lack of care we may have exercised in handling your account;

[...]

If you report to us that an unauthorized transaction has occurred on your account, we may require you to confirm your report in writing. We may also require that you give us a statement, under penalty of perjury, about the facts and circumstances relating to your report and provide such other information and proof as we may reasonably request. If you assert a claim regarding a problem, you must cooperate

> with us in the investigation and prosecution of your claim and any attempt to recover funds. You also agree to assist us in identifying and in seeking criminal and civil penalties against the person responsible. You must file reports and complaints with appropriate law enforcement authorities. If you fail or refuse to do these things, we will consider your failure or refusal to be your ratification of the defect in the statement or item, unauthorized transaction or other problem and your agreement that we can charge the full amount to your account.

Id., at 43.

66. These provisions are and were reasonably understood by Plaintiff to mean that Plaintiff would not be liable for Zelle transfers effectuated by fraud. But BofA unilaterally and unreasonably decided "fraud" only means transfers initiated by someone other than the accountholder.

C. The Bank Employee Impersonation or Me-to-Me Scam

67. This Action concerns a specific form of fraud that is assisted and enabled—even if unwittingly—by the Bank.

68. So-called "me-to-me" fraud (or bank employee impersonation fraud) occurs when a scammer—often from a bank caller ID—tells the consumer that his or her bank account was compromised, and persuades the person to send money to what appears to be himself or herself using Zelle. In reality, the scammer has linked the consumer's cellphone to a fraudulent Zelle account.

69. Another common bank employee impersonation scam involves a scammer who alerts the bank customer to suspicious account activity and offers to help prevent the alleged fraud by advising that the accountholder transfer money to a different bank account. Unsuspecting Zelle users, tricked into making a fraudulent transfer, in many cases send hundreds or thousands of dollars to fraudsters.

70. This scam cannot succeed without the assistance of the Bank, specifically the Bank's mistaken and negligent linking of a legitimate BofA accountholder's cellphone number to scammer's account. That error is the key link that allows this scam to take place.

71. BofA had the tools and information to stop this incorrect linkage, but failed to do so.

72. Combined with the porous and dangerous Zelle architecture and design, as discussed above, Bank of America aided and abetted the bank impersonation scam that afflicted Plaintiff and thousands of others.

73. Bank of American should have prevented this error on the front end or, at the very least, correct this error after it occurred. It failed to do either.

74. As one consumer advocate has stated: "If a bank mistakenly links your cellphone number to a scammer's account, that's an error that should be corrected and you should be able to get your money back," said Lauren Saunders, associate director at the National Consumer Law Center.

D. Bank of America Is Required to Follow EFTA Requirements and It Fails to Do So

75. The Electronic Fund Transfer Act requires banks to reimburse customers for losses on transfers that were "initiated by a person other than the consumer without actual authority to initiate the transfer."[3]

76. An unauthorized Electronic Fund Transfer ("EFT") is an EFT from a consumer's account initiated by a person other than the consumer without actual authority to initiate the transfer and from which the consumer receives no benefits. 12 C.F.R. § 1005.2(m).

[3] 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/ (last accessed June 6, 2022).

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

78. According to the Consumer Financial Protection Bureau ("CFPB"), "If a consumer has provided timely notice of an error under 12 CFR 1005.11(b)(1) and the financial institution determines that the error was an unauthorized EFT, the liability protections in Regulation E section 1005.6 would apply."[4]

79. Recent CFPB guidance on unauthorized electronic fund transfers indicates person-to-person payments are electronic fund transfers, such as transactions made with Zelle, and trigger "error resolution obligations" to consumers to protect them from situations where they are fraudulently induced to initiate an unauthorized electronic transfer from a third-party.[5]

80. The CFPB has made it clear that a transaction that is fraudulently induced by a third party is an unauthorized electronic fund transfer subject to the limitations of liability in 12 C.F.R. § 1005.6.[6]

81. Even so, BofA has not reversed or refunded all funds of Plaintiff's disputed and unauthorized transactions, though obligated to do so.

82. Because banks, such as BofA, fail to protect consumers as widespread "fraud flourishes" on Zelle, Senators Elizabeth Warren, Robert Menendez and Jack Reed sent a letter to the CEO of Zelle noting:

> The Consumer Financial Protection Bureau previously clarified that Regulation E of the Electronic Fund Transfer Act protected victims of fraudulent money

---

[4] *Id.*
[5] *Id.*
[6] 12 C.F.R. § 1005.6 (Regulation E), Comment 2(m)-3, https://www.consumerfinance.gov/rules-policy/regulations/1005/interp-2/#2-k-Interp-1 ("An unauthorized [electronic fund transfer] includes a transfer initiated by a person who obtained the access device from the consumer through fraud") (last accessed June 6, 2022).

> transfers, **including those who were "induced" into transferring the money themselves,** while the FDIC issued a report in March 2022 finding that both the banks and the platform—in this case Zelle—were held responsible for fraudulent electronic transfers through Regulation E.

Senator Warren Letter to Zelle on Scams and Fraud (April 20, 2022), (https://www.warren.senate.gov/imo/media/doc/2022.04.29%20Letter%20to%20Early%20Warning%20Systems%20LLC.pdf) (last accessed June 6, 2022) (emphasis added).

83. A recent Wall Street Journal article discussed potential CFPB action regarding fraud protections on Zelle, noting that congressional officials "complain that banks aren't doing enough to help customers duper into making fraudulent payments," like Plaintiff, but the CFPB's forthcoming guidance is expected to address banks' liabilities in these circumstances "by maintaining that fraudulently induced transactions, *even those approved by the consumer*, are considered unauthorized."[7]

84. This makes sense. In the digital age, where it only takes a username or phone number to transfer money in seconds, it's "antiquated" for reimbursement to hinge on whether a consumer or fraudster taps the send button. As the Senate Banking Committee told the CFPB Director Rohit Chopra:

> If a bank permits a scammer or fraudster onto the platform, then that bank should naturally bear some responsibility when its own customer uses a bank-provided payment service to rip off others—rather than telling customers that it is their fault for being victimized.

Senate Banking Committee Letter to CFPB re Frauds and Scams Zelle (July 20, 2022), https://www.menendez.senate.gov/imo/media/doc/letter_to_cfpb_regarding_zelle.pdf (last accessed July 21, 2022).

85. Unfortunately, BofA regularly fails to consider fraudulently induced Zelle transactions as "unauthorized" electronic transfers, thus depriving accountholders of their rights

[7] *CFPB to Push Banks to Cover More Payment-Services Scams*, The Wall Street Journal (July 18, 2022), https://www.wsj.com/articles/consumer-bureau-to-push-banks-to-refund-more-victims-of-scams-on-zelle-otherservices-11658235601 (last accessed July 21, 2022).

to be reimbursed for such fraudulent transfers, even where the losses are timely reported by consumers.

86. As one U.S. Senator said to CEOs of some of the banks that own Zelle: "Zelle is not safe. You built the system, you profit from every transaction on the system and you tell people that it is safe. But when someone is defrauded, you claim that's the customer's problem," said Senator Elizabeth Warren, during a Senate Banking Committee hearing in September, 2023.

E. Plaintiff Wolf's Experience

87. When Plaintiff signed up for Zelle she was not informed that Zelle's service had a significant "catch" and that significant monetary losses could result from signing up for the service—or that those losses almost never are reimbursed by users' banks or credit unions.

88. For example, on June 11, 2022, a fraudster masquerading as a BofA representative transferred $3,500 from Plaintiff's personal bank account using the Zelle service.

89. On or about June 11, 2022, Plaintiff received an incoming call identified as Bank of America from phone number 1-800-432-1000 which Plaintiff recognized as the Bank's customer service number found on the back of BofA debit and credit cards.

90. Upon answering, the fraudster introduced themselves as a representative from Bank of America's fraud department. The fraudster claimed the call was to alert Plaintiff of suspected "fraudulent activity" on Plaintiffs account; the "fraudulent activity" was purported to be two transfers of $1,500.00 and $2,000.00 totaling $3,500.00. The fraudster gave Plaintiff assurances and guided her through the process of "reversing" the fraudulent activity debited against her bank account.

91. In order to restore her account funds, the fraudster instructed Plaintiff to make two Zelle transfers for the same amount of the "fraudulent activity" (i.e., $1,500.00 and $2,000.00).

92. The fraudster never asked Plaintiff to disclose personal information such as her account passwords or pins.

93. The fraudster walked Plaintiff through the process of adding a new Zelle recipient in her Bank of America mobile app and reassured Plaintiff that taking these steps will restore her account funds. As instructed, Plaintiff sent $1,500.00 to the new Zelle recipient the fraudsters duped Plaintiff into adding.

94. Next, Plaintiff repeated the same steps for the second transfer in the amount of $2,000.00.

95. Upon sending the second transfer, Plaintiff began to grow weary and she asked to speak with the fraudster's supervisor. The fraudster put Plaintiff on hold and then disconnected the call.

96. Immediately, Plaintiff called the BofA customer service number who, after hearing Plaintiff recount her experience with the fraudster impersonating as a BofA agent, informed Plaintiff that she had fallen victim to a scam.

97. Despite Plaintiff timely alerting BofA of the fraud, BofA refused to reimburse her for the loss.

CLASS ALLEGATIONS

98. Pursuant to Rule 23 of the North Carolina Rules of Civil Procedure, Plaintiff brings this action individually and as representatives of all those similarly situated, on behalf of the below-defined Classes:

> **Nationwide Class:**
> All persons with a BofA account who were subject to a BofA employee impersonation scam or me-to-me scam and incurred unreimbursed losses due to fraud using the Zelle service.

California Class:
All California persons with a BofA account who were subject to a BofA employee impersonation scam or me-to-me scam and incurred unreimbursed losses due to fraud using the Zelle service.

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

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

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

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

a) Whether Defendant's representations and omissions about the Zelle service are false, misleading, deceptive, or likely to deceive;

b) Whether Defendant failed to disclose the risks of using the Zelle service;

c) Whether Plaintiff and the Class members were damaged by Defendant's conduct;

d) Whether Defendant's actions or inactions violated the consumer protection statute invoked herein;

e) Whether Defendant's actions or inactions violated the EFTA; and

f) Whether Plaintiff is entitled to a preliminary and permanent injunction enjoining Defendant's conduct.

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

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

105. **Adequacy of Representation:** Plaintiff is an adequate class representative because she is fully prepared to take all necessary steps to represent fairly and adequately the interests of the members of the Classes, and because her interests do not conflict with the interests of the other Class members she seeks to represent. Moreover, Plaintiff's attorneys are ready, willing, and able to fully and adequately represent Plaintiff and the members of the Classes. Plaintiff's attorneys are experienced in complex class action litigation, and they will prosecute this action vigorously.

106. **Superiority:** The nature of this action and the claims available to Plaintiff and members of the Classes make the class action format a particularly efficient and appropriate procedure to redress the violations alleged herein. If each Class member were required to file an individual lawsuit, Defendant would necessarily gain an unconscionable advantage since it would be able to exploit and overwhelm the limited resources of each individual Plaintiff with its vastly superior financial and legal resources. Moreover, the prosecution of separate actions by individual Class members, even if possible, would create a substantial risk of inconsistent or varying verdicts or adjudications with respect to the individual Class members against Defendant, and which would establish potentially incompatible standards of conduct for Defendant and/or legal determinations with respect to individual Class members which would, as a practical matter, be dispositive of the interests of the other Class members not parties to adjudications or which would substantially impair or impede the ability of the Class members to protect their interests. 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
North Carolina Unfair Trade Practices Act ("NCUTPA")
N.C. Gen. Stat. Ann. §§ 75-1.1, *et seq.*
(Asserted on Behalf of Plaintiff and the Nationwide Class)

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

108. The North Carolina Unfair Trade Practices Act ("NCUTPA"), makes unlawful "unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce." N.C. Gen. Stat. Ann. § 75-1.1(a).

109. BofA advertised, offered, or sold goods services in North Carolina and engaged in trade or commerce directly or indirectly affecting the people of North Carolina, as defined by N.C.

Gen. Stat. Ann. § 75-1.1(b), by offering the Zelle money transfer services through its website and mobile app.

110. As alleged herein, BofA, violated the NCUTPA by knowingly and intentionally representing in marketing materials that it provides "safe" and "secure" money transfer services via Zelle through its website and mobile app.

111. Moreover, as alleged herein, BofA, knowingly and intentionally concealed and failed to disclose material facts regarding Zelle in violation of the NCUTPA. Specifically, BofA omitted from all its marketing the material security risks of using the Zelle service, including the risk of fraud and the risk that fraudulent losses will never be reimbursed by BofA as a matter of secret policy due to its unilateral and unreasonable decision that "fraud" only means transfers initiated by someone other than the accountholder.

112. BofA's practice of refusing to reimburse its accountholders' for fraudulent Zelle transactions is deceptive and unfair because of BofA's marketing representations that Zelle transfers from consumers' accounts are safe and secure and because of its marketing and contractual promises which indicate accountholders will not be liable for fraudulent transfers, if they timely report the fraud.

113. By knowingly and intentionally misrepresenting, omitting, concealing, and failing to disclose material facts regarding use of the Zelle service, as detailed above, BofA engaged in one or more unfair or deceptive business practices prohibited by the NCUTPA.

114. Defendant's misrepresentations and omissions regarding the Zelle service were made to Plaintiff and the Nationwide Class members in a uniform manner.

115. Defendant's unfair or deceptive acts or practices, including its misrepresentations, concealments, omissions, and suppression of material facts, as alleged herein, had a tendency or

capacity to mislead and create a false impression in consumers' minds, and were likely to and, in fact, did deceive reasonable consumers, including Plaintiff and the Nationwide Class members.

116. The facts regarding Defendant's Zelle service that Defendant knowingly and intentionally misrepresented, omitted, concealed, and/or failed to disclose would be considered material by a reasonable consumer, and they were, in fact, material to Plaintiff and the Nationwide Class members.

117. The harm to Plaintiff and the Class outweighs the utility of BofA's practices. There were reasonably available alternatives to further BofA's legitimate business interests, other than the misleading and deceptive conduct described herein.

118. Defendant's business practices have misled Plaintiff and the proposed Nationwide Class and will continue to mislead them in the future.

119. Plaintiff and Nationwide Class members relied on Defendant's misrepresentations.

120. Plaintiff and Nationwide Class members had no way of discerning that Defendant's representations were false and misleading, or otherwise learning the facts that Defendant had concealed or failed to disclose. Plaintiff and Nationwide Class members did not, and could not, unravel Defendant's deception on their own.

121. Had Plaintiff known the true risks of using the Zelle service, she never would have signed up for and used the Zelle service through BofA's website and mobile app.

122. BofA's actions affected commerce in North Carolina and nationwide, as many BofA customers incurred fraud losses via Zelle.

123. As a direct and proximate result of Defendant's deceptive and unfair conduct, Plaintiff and Nationwide Class members suffered and will continue to suffer actual damages.

Defendant's deceptive and unfair conduct is ongoing and present a continuing risk of future harm to Plaintiff and the Nationwide Class.

124. Plaintiff and the Nationwide Class members seek an order enjoying Defendant's unfair and deceptive acts or practices in violation of the NCUTPA and awarding actual damages, costs, attorneys' fees, and any other just and proper relief available pursuant to the NCUTPA.

SECOND CAUSE OF ACTION
California's Unfair Competition Law ("UCL")
Cal. Bus. & Prof. Code §§ 17200, *et seq.*
(Asserted on Behalf of Plaintiff and the California Class)

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

126. The UCL defines "unfair business competition" to include any "unlawful, unfair, or fraudulent" act or practice, as well as any "unfair, deceptive, untrue or misleading" advertising. Cal. Bus. & Prof. Code § 17200.

127. 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.

"Deceptive Prong"

128. A business act or practice is "fraudulent" under the UCL if it is likely to deceive members of the public.

129. Defendant's practices, as described herein, constitute "fraudulent" business practices in violation of the UCL because, among other things, Defendant's marketing regarding Zelle indicates the Bank will protect against fraudulent losses incurred using the Zelle service. Moreover, Defendant concealed the security risks of using the Zelle service, including the risk of fraud and the risk that fraudulent losses will never be reimbursed by BOA as a matter of secret policy, is a practice that is likely to deceive a consumer acting reasonably under the circumstances, to the consumer's detriment.

"Unfair" Prong

130. A business 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 practices against the gravity of the harm to the alleged victims.

131. Defendant's actions constitute "unfair" business practices because, as alleged above, they declined to reverse fraudulent charges on the accounts of Plaintiff and California Class Members, despite marketing representations, contract promises, and statutory obligations pursuant to EFTA.

132. The harm to Plaintiff and California Class Members grossly outweighs the utility of Defendant's practices as there is no utility to practices of Defendant.

"Unlawful" Prong

133. A business act or practice is "unlawful" under the UCL if it violates any other law or regulation.

134. Defendant's acts and practices alleged above constitute unlawful business acts or practices as they have violated the plain language of EFTA as described in Plaintiff's Fourth Cause of Action below.

135. The violation of any law constitutes as "unlawful" business practice under the UCL.

136. These acts and practices alleged were intended to or did result in violations of EFTA.

137. Defendant has and will continue to unlawfully deny the transaction disputes of Plaintiff, the California Class, and the public by claiming that said disputed transactions are "authorized," even though said transactions are actually "unauthorized," as that term is defined by EFTA and applicable regulations. Consequently, the practices of BofA constitute unfair and unlawful business practices within the meaning of the UCL.

138. Pursuant to the UCL, Plaintiff and the California Class are entitled to preliminary and permanent injunctive relief and order Defendant to cease this unfair and unlawful competition, as well as disgorgement and restitution to Plaintiff and the Class of all the revenues associated

with this unfair and unlawful competition, or such proton of said revenues as the Court may find applicable.

139. Pursuant to the UCL, Plaintiff and the California Class are entitled to preliminary and permanent injunctive relief and an order requiring Defendant to cease this unfair and unlawful competition, as well as disgorgement and restitution to Plaintiff and the California Class of all revenues associated with this unfair and unlawful competition, or such portion of said revenues as the Court may find applicable.

THIRD CAUSE OF ACTION
Violation Of California's False Advertising Law ("FAL")
Cal. Bus. & Prof. Code §§ 17500, *et seq.*
(Asserted on Behalf of Plaintiff and the California Class)

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

141. California's False Advertising Law ("FAL"), Cal. Bus. & Prof. Code § 17500, states that "[i]t is unlawful for any ... corporation ... with intent ... to dispose of ... personal property ... to induce the public to enter into any obligation relating thereto, to make or disseminate or cause to be made or disseminated ... from this state before the public in any state, in any newspaper or other publication, or any advertising device, or by public outcry or proclamation, or in any other manner or means whatever, including over the Internet, any statement...which is untrue or misleading and which is known, or which by the exercise of reasonable care should be known, to be untrue or misleading...."

142. Defendant's material misrepresentations and omissions alleged herein violate Bus. & Prof. Code § 17500.

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

144. Pursuant to Business & Professions Code §§ 17203 and 17500, Plaintiff and the members of the California Class, on behalf of the general public, seeks an order of this Court

enjoining Defendant from continuing to engage, use, or employ their practice of misrepresenting the Zelle service.

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

146. Additionally, Plaintiff the members of the California Class seek an order requiring Defendant to pay attorneys' fees pursuant to Cal. Civ. Code § 1021.5.

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

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

148. 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).

149. 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).

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

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

152. "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).

153. 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).

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

155. Pursuant to the EFTA, an error includes "an unauthorized electronic fund transfer." Id. § 1693f(f).

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

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

158. According to the CFPB, when a third party fraudulently induces a consumer into sharing account access information that is used to initiate an EFT from the consumer's account, that transfer meets Regulation E's definition of an unauthorized EFT.

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

160. Here, Plaintiff and Members of the Classes were fraudulently induced by third-party scammers impersonating BofA representatives to make unauthorized money transfers from their BofA accounts.

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

162. Plaintiff and Members of the Classes notified Defendant Bank of America, N.A. of these errors within sixty (60) days of their appearances on their accounts.

163. As a direct and proximate result of Defendant's conduct, Plaintiff and Members of the Classes were unable to reclaim the account funds taken from scammers from unauthorized EFTs.

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

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

166. Defendant refused to reverse or refund funds to Plaintiff and Members of the Classes.

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

FIFTH CAUSE OF ACTION
Breach of Contract Including Breach of the Covenant of Good Faith and Fair Dealing (Asserted on Behalf of Plaintiff and the Classes)

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

169. Plaintiff and members of the Classes contracted with Defendant for checking account services, as embodied in the Account Disclosures.

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

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

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

173. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—not merely the letter—of the bargain. Put differently, the parties to a contract are mutually obligated to comply

with the substance of their contract in addition to its form. Evading the spirit of the bargain and abusing the power to specify terms constitute examples of bad faith in the performance of contracts.

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

175. Defendant breached the covenant of good faith and fair dealing when it failed to fairly investigate reported fraudulent, unauthorized transactions on the Zelle money transfer service and failed to reimburse accountholders for fraud-induced losses incurred using the Zelle, and unilaterally adopting an unreasonable definition of "unauthorized" where "fraud" only means transfers initiated by someone other than the accountholder.

176. Each of Defendant's actions were done in bad faith and was arbitrary and capricious.

177. Plaintiff and members of the Classes have performed all, or substantially all, of the obligations imposed on them under the contract.

178. Plaintiff and members of the Classes have sustained damages as a result of Defendant breaches of the contract and covenant of good faith and fair dealing.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the Classes, demands a jury trial on all claims so triable and judgment as follows:

A. Certifying the proposed Classes, appointing Plaintiff as representative of the Classes, and appointing counsel for Plaintiff as lead counsel for the respective Classes;

B. Declaring that Defendant's policies and practices as described herein constitute a violation of the state consumer protection statutes invoked herein, breach of contract and a breach of the covenant of good faith and fair dealing, and/or BofA's conduct is a violation of the Electronic Funds Transfer Act.

C. Enjoining Defendant from the unlawful conduct as described herein;

D. Awarding restitution of all monies Defendant acquired as a result of the wrongs alleged herein in an amount to be determined at trial;

E. Compelling disgorgement of the ill-gotten gains derived by Defendant from its misconduct;

F. Awarding actual and/or compensatory damages according to proof;

G. Punitive and exemplary damages;

H. Treble damages and attorneys' fees as provided by law;

I. Awarding pre-judgment interest at the maximum rate permitted by applicable law;

J. Reimbursing all costs, expenses, and disbursements accrued by Plaintiff in connection with this action, including reasonable attorneys' fees, costs, and expenses, pursuant to applicable law and any other basis; and

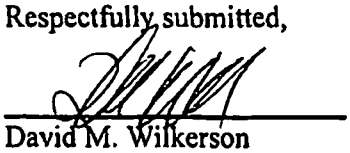
K. Awarding such other relief as this Court deems just and proper.

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: October 12, 2022

Respectfully submitted,



David M. Wilkerson
NC State Bar No. 35742
THE VAN WINKLE LAW FIRM
11 North Market Street
Asheville, NC 28801
Phone: 828-258-2991
Fax: 828-257-2767
Email: dwilkerson@vwlawfirm.com

Counsel for Plaintiff and the Proposed Class