IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

MELINDA GLAVIN, individually and on behalf of all others similarly situated, Plaintiff, v. JPMORGAN CHASE BANK, N.A. D/B/A CHASE BANK, JPMORGAN CHASE & CO., AND EARLY WARNING SERVICES, LLC D/B/A ZELLEPAY.COM, Defendants.	Case No.: **COMPLAINT – CLASS ACTION**

Upon personal knowledge as to her own acts and status, and based upon her investigation, her counsel's investigation, and information and belief as to all other matters, Plaintiff Melinda Glavin ("Ms. Glavin" or "Plaintiff") brings this complaint ("Complaint") on behalf of herself and all others similarly situated against Defendants JPMorgan Chase Bank, N.A., d/b/a Chase Bank and JPMorgan Chase & Co. (collectively "Chase"), and Early Warning Services, LLC d/b/a Zellepay.com ("Zelle") (collectively "Defendants") and alleges as follows:

I. INTRODUCTION

1. Plaintiff Melinda Glavin is a victim of fraudulent activity targeting customers of Chase in connection with the Zelle mobile application, resulting in $6,500 being debited from her checking account without her authorization.

2. Ms. Glavin's Chase account was debited $6,500 in June 2022 through her Zelle application, which was linked to her Chase checking account. Chase initially provisionally refunded the stolen amount from Ms. Glavin's account, but after a brief investigation, Chase reversed its initial

decision and refused to refund any of the $6,500 in stolen funds because it claimed that the fraudulent payments "came from her phone."

3. This chain of events is well-known to Defendants. Chase partially owns Zelle, and Chase installs Zelle in the Chase mobile banking app automatically. However, Defendants have not taken adequate steps to protect consumers from Zelle fraud, which often results in substantial losses to individual consumers and customers of Chase.

4. When Congress enacted the Electronic Fund Transfer Act ("EFTA"), 15 U.S.C. § 1693 et seq., it established the rights, liabilities, and responsibilities of participants in electronic fund transfer systems. The EFTA "requires financial institutions to adopt certain practices respecting such matters as transacting accounting, and **error resolution**, requires financial institutions and others to have certain procedures for preauthorized transfers, and sets liability limits for losses caused by unauthorized transfers."[1] (emphasis added).

5. In enacting the EFTA, Congress intended to "provide a basic framework establishing the rights, liabilities, and responsibilities of participants in electronic fund and remittance transfer systems." *Id*. § 1693(b). "The primary objective of [the EFTA] is the provision of **individual consumer rights**." *Id*. (emphasis added).

6. The EFTA is implemented by Regulation E, a federal regulatory scheme designed to protect consumers when engaging in electronic transfers of their money. 15 U.S.C. § 1693(a), 12 CFR § 1005.3(a).

[1] https://www.ftc.gov/legal-library/browse/statutes/electronic-fund-transfer-act (last accessed Feb. 28, 2023).

7. The Dodd-Frank Act transferred rule-making authority under the EFTA from the Federal Reserve Board to the Consumer Financial Protection Bureau ("CFPB").[2] With it, the CFPB obtained authority to supervise and enforce EFTA compliance as well as implementing regulations, including Regulation E.[3]

8. The regulation defines an "electronic fund transfer" ("EFT") as 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 CFR § 1005.3(b)(1).

9. Defendants are financial institutions covered by the EFTA and Regulation E. Such "financial institutions" include persons who issue "access devices" and agree with consumers to provide EFT services. 12 CFR § 1005.2(i). Regulation E defines "access devices" to mean a card, code, or other means of access to a consumer's account that may be used by the consumer to initiate EFTs.

10. When users activate a Zelle account through their Chase mobile banking application, a code is sent to their phone via text message, which is then used to link the Zelle account and phone number associated with their Chase bank account. This constitutes an access device under Regulation E and therefore subjects both Chase and Zelle to the federal regulations pertaining to financial institutions.

11. Subsection 1963(f) of the EFTA requires that financial institutions meet specific requirements when consumers make reports of errors in their accounts. 15 U.S.C. § 1693(f). These requirements include but are not limited to conducting an investigation of the error and correcting

[2] https://www.cfpaguide.com/portalresource/Exam%20Manual%20v%202%20-%20EFTA.pdf (last accessed Feb. 28, 2023).
[3] *Id*.

the error, including crediting of interest where applicable, as well as providing an explanation of any findings of absence of error to consumers. 15 U.S.C. § 1693f(a) – (d).

12. Specifically, when it comes to unauthorized transfers, a consumer will only be liable if the means of access to the account was *authorized* by the account holder. 15 U.S.C. § 1693g(a). In determining whether a transaction was authorized or not, the financial institution bears the burden of proof for establishing the transfer was authorized. 15 U.S.C. § 1693g(b).

13. Zelle has repeatedly and systematically avoided this liability imposed on it by the EFTA by conducting cursory investigations and determining transactions to have been authorized based only on the fact that the transactions appear to have been sent from the consumer's access device, even if they were obtained by fraud.

14. Zelle and the banks that own it are on average reimbursing only 50% of fraud claims reported by consumers who have had money fraudulently transferred from their accounts. Pursuant to the EFTA, Zelle and Chase are mandated to conduct thorough investigations of any claim of a transfer error, to correct the error if found to be unauthorized, and to provide an explanation as to why a transfer was found to be authorized despite a consumer's claim. Defendants have failed to abide by these requirements, which cost consumers over $440 million in 2021 alone.[4]

II. JURISDICTION AND VENUE

15. This Court has original subject matter jurisdiction pursuant to 28 U.S.C. § 1331 because this case arises out of violations of federal law under the EFTA, 15 U.S.C. § 1693 §§ *et seq*. Jurisdiction of this Court arises pursuant to 28 U.S.C. §§ 1331 and 1367 for supplemental

[4] Allison Morrow, Zelle Fraud is Rising. And Banks Aren't Coming to the Rescue, CNN Business (Oct. 3, 2022), https://www.cnn.com/2022/10/03/business/nightcap-zelle-fraud-warren-investigation/index.html.

jurisdiction over the Pennsylvania state law claims arising from the same transactions or occurrences that form the basis of the federal EFTA claim.

16. This Court has personal jurisdiction over Defendants pursuant to 18 U.S.C. § 1965(a) because Defendants were and remain engaged in the marketing, selling, and providing of Defendants' services in the Commonwealth of Pennsylvania. A substantial portion of the wrongdoing alleged in this Complaint took place in Pennsylvania; Defendants conduct business in Pennsylvania and otherwise avail themselves of the protections and benefits of Pennsylvania law through the promotion, marketing, and provided services of Defendants' products and services in the Commonwealth; and this action arises out of or related to these contacts because Plaintiff and the Class (defined below) received and used the services in Pennsylvania.

17. Venue is proper pursuant to 28 U.S.C. § 1391(b) because (1) Defendants transact business within this judicial district and because Plaintiff was a resident of Wayne, Pennsylvania in Delaware County at all times relevant to these claims such that a substantial part of the events giving rise to Plaintiff's causes of action against Defendant occurred while Plaintiff resided in this District; and (2) Defendants' contacts with this District are sufficient to subject them to personal jurisdiction within this District.

III. PARTIES

18. Plaintiff is, and at all times relevant herein has been, a resident of Pennsylvania, County of Delaware, in this District.

19. Defendant JPMorgan Chase & Co. is a diversified financial services company headquartered in New York City, New York that provides banking, insurance, investments, mortgage banking, and consumer finance through banking stores, the Internet, and other

distribution channels to customers, businesses, and other institutions in all 50 states and in other countries. It is the largest bank in the United States.

20. JPMorgan Chase Bank, N.A., d/b/a Chase Bank, constitutes the consumer and commercial banking subsidiary of the U.S. multinational banking and financial services holding company, JP Morgan Chase & Co.

21. JPMorgan Chase Bank exercises specific and financial control over the operations of Chase Bank, dictates the policies, procedures, and practices of Chase Bank, exercises power and control over the specific activities upon which the claims herein are based, and is the ultimate recipient of the unreimbursed transactions described herein.

22. Plaintiff is informed and believes, and thereon alleges, that Chase Bank is, and at all times mentioned herein was, a national bank association chartered under the laws of the United States with its primary place of business in New York City, New York.

23. Defendant Zelle is an instant payment services business owned by seven large banks in the United States, one of which is JPMorgan Chase & Co. Zelle earns profit by facilitating payments with participating banks, including Chase.

IV. FACTUAL ALLEGATIONS

Background on Zelle Fraud

24. Zelle was created in 2017 by the largest banks in the United States: JPMorgan Chase, Bank of America, Capital One, PNV, Trust, U.S. Bank, and Wells Fargo. Zelle enables digital money transfers between members of different banks and is included in these banks' mobile applications. Zelle is now the most popular money transfer service in the United States, surpassing its

competitor, Venmo. In 2021, Zelle processed $290 billion in volume, compared to only $230 billion by Venmo, and $175 billion by Block, Inc.'s Cash App.[5]

25. Zelle's website describes the system as a peer-to-peer payment platform and "a great way to send money to friends and family, even if they bank somewhere different than you do. Plus, it's in a lot of banking apps, probably yours!"[6]

26. Zelle uses phone number-based accounts to connect a user's phone to their Chase banking account with transfers requiring no other information than the user on the other end of the transaction's cell phone number. "Once you're enrolled with Zelle, all you need is an email address or U.S. mobile phone number to send money to friends and family straight from your banking app."[7]

27. Zelle also boasts of the immediacy of Zelle payments, while failing to mention that the immediacy of the transactions means there is no way for a user to retract a payment. When using Zelle, the money is taken from one checking account and moved to another almost instantaneously. "If your recipient is already enrolled with Zelle, the money will go directly into their bank account, typically in minutes[]."[8]

28. Though the immediacy of Zelle's service has made it a favorite among consumers, it has also made it a favorite among fraudsters, thieves, and hackers. On April 29, 2022, three U.S.

[5] Emily Mason, Despite a Late Start, Bank-Owned Zelle Moves More Money Than Venmo and Cash App Combined, Forbes.com, https://www.forbes.com/sites/emilymason/2022/09/08/despite-a-late-start-bank-owned-zelle-moves-more-money-than-venmo-and-cash-app-combined/?sh=7001cb9f9d3f (last accessed Jan. 25, 2023).
[6] https://www.zellepay.com/how-it-works (last accessed Feb. 22, 2023).
[7] *Id*.
[8] *Id*.

senators, Elizabeth Warren, Robert Menendez, and Jack Reed, wrote to the bank owners of Zelle calling out the banks for failing to do enough to prevent fraud on their peer-to-peer system.[9]

29. The letter from the Senators stated, "It is imperative that the banks that created, own and offer the service do more to protect consumers from the fraud and scams that are being perpetrated through the platform."[10]

30. The letter also explained that Zelle's integration into banking mobile applications leads consumers to believe they have the same protections against fraud and unauthorized transactions as they have when using bank-issued credit or debit cards.[11] In the case of ordinary credit or debit card transaction, the networks that process these transactions have implemented robust fraud protections, which require the connected banks to be liable in the case of fraud, stolen cards, or chargebacks.[12] These same banks, however, do not follow similar fraud protection policies for Zelle transactions.

31. In 2022, Senator Warren reviewed bank data and found the data suggested "that even the bulk of unauthorized cases are going unpaid. For example: PNC Bank indicated that its customers reported 10,683 cases of unauthorized payments totaling over $10.6 million. It refunded only 1,495 cases, totaling $1.46 million."[13]

32. Since 2017, Zelle has claimed that only 0.09% of transactions on the payment app are fraudulent. However, even if that were true, in the scheme of $490 billion in revenue, those fraudulent transactions would amount to as much as $440 million in a year.[14]

---

[9] *Supra* note 1.
[10] *Id*.
[11] *Id*.
[12] *Id*.
[13] *Supra* note 4.
[14] *Id*.

33. Banks, however, including Chase, are aware of the widespread fraud on Zelle but are doing virtually nothing to stop it and little to nothing to help consumers get their money back.

34. In response to Senator Warren's report, Zelle released a statement addressing the allegations and claimed, "Tens of millions of consumers use Zelle without incident, with more than 99.9% of payments completed without any report of fraud or scam."[15] The statement continued, "Zelle is the safest peer-to-peer network."[16]

35. Despite Defendants being acutely aware of this fraud, banks like Chase, and Zelle itself, have not adequately informed and educated consumers about the risks of using Zelle's system, a service in which Defendants have a financial interest.

Zelle Advertised Its Service as a Safe Way to Send Money and Promised to Reimburse Fraudulent Transactions

36. Defendant Zelle touts its service as "fast, safe, and easy."[17] These misrepresentations are made multiple times to consumers throughout Zelle's website.

37. Under Zelle's Security page on its website, Zelle states "authentication and monitoring features are in place to help make your payments secure when you're sending and receiving money."[18] Similarly, Zelle's "Frequently Asked Questions" page misleadingly repeats the aforementioned language from the home page and continues, "So whether you're using the Zelle app or using Zelle through your bank or credit union's mobile app or online banking, you'll have peace of mind."[19] The website even includes a section describing the differences in Zelle and Chase Online Bill Pay and only lists a cursory description of the minor differences in services, while

[15] *Id*.
[16] *Id*.
[17] https://www.zellepay.com/how-it-works (last accessed Apr. 12, 2023).
[18] https://www.zellepay.com/security (last accessed Apr. 12, 2023).
[19] https://www.zellepay.com/faq/my-information-secure (last accessed Apr. 12, 2023).

conveniently omitting the lack of protections for consumers when using Zelle. "Zelle is a person-to-person payment service that lets you send and receive money from anyone with a U.S. bank account using an email address or mobile number. You can use Chase Online Bill Pay for one-time and scheduled payments for your recurring monthly bills (for example, your rent or mortgage, utilizes, credit card bills and car payments)."[20]

38. Zelle's most obvious misrepresentation is found on its "Financial Education" page of the website under the headline "Understanding Fraud & Scams."[21] The page describes the difference between authorized and unauthorized use, synonymous with the Regulation E definition, but then promises customers coverage and protection against unauthorized transactions:

> If someone gained access to your account, and stole money or sent it without your permission, this could be defined as fraud. Immediately report suspected **unauthorized activity** to your financial institution. Because you did NOT authorize a payment, you are typically able to get your money back after reporting the incident.[22]

Zelle's own website instructs consumers on how to seek reimbursement for fraudulent charges on their accounts, and yet has failed to follow through on its promises.

[20] https://www.chase.com/personal/zelle (last accessed Apr. 12, 2023).
[21] https://www.zellepay.com/financial-education/pay-it-safe/understanding-fraud-scams (last accessed Apr. 12, 2023).
[22] *Id*. (emphasis in original).

FRAUD

If someone gained access to your bank account and made a payment with Zelle® without your permission, and you weren't involved in any way with the transaction, this is typically considered fraud since it was unauthorized activity. If someone gained access to your account, and stole money or sent it without your permission, this could be defined as fraud. Immediately report suspected **unauthorized activity** to your financial institution. Because you did NOT authorize a payment, you are typically able to get your money back after reporting the incident.

Fraud

Someone gained **unauthorized** access to your money.

EXAMPLE

Someone gained access to your bank account without your permission. You never authorized or were involved in the transaction.

WHAT TO DO

Immediately report suspected unauthorized activity to your financial institution.

CAN YOU GET YOUR MONEY BACK?

Because you **did not authorize a payment**, you are typically able to get your money back.

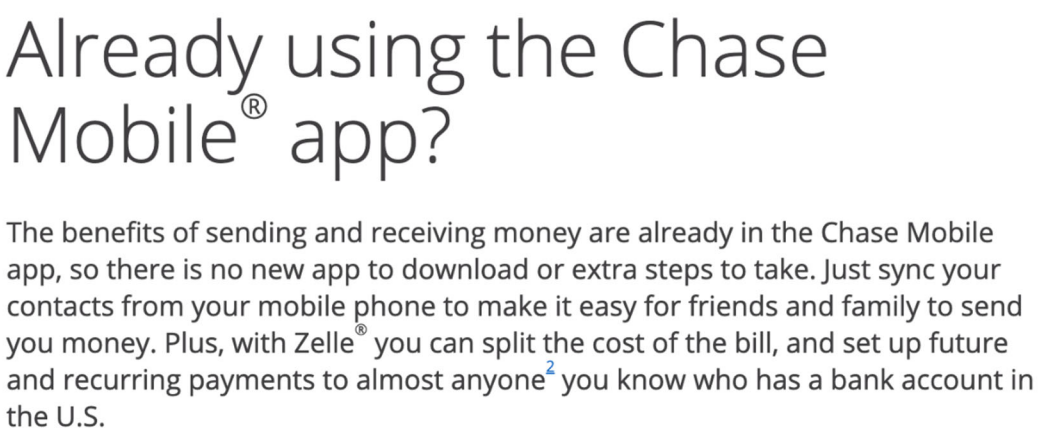
39. Chase's website contains a special page dedicated to its partnership with Zelle with three bolded terms describing Zelle through Chase as "Fast, Convenient, Secure." [23] Under the "secure" headline, Chase claims "Your account information stays protected. You won't see the other person's bank account info, and they won't see yours."[24]

Secure

Your account information stays protected. You won't see the other person's bank account info, and they won't see yours.

40. Additionally the website continues with perhaps the most misleading statement: "The benefits of sending and receiving money are already in the Chase Mobile app, so there is no new app to download or extra steps to take."[25] Defendants knew that the benefits of Chase banking did not apply to Zelle payments, but continued to portray them as one intertwined service.

[23] https://www.chase.com/personal/zelle (last accessed Apr. 12, 2023).
[24] *Id*.
[25] *Id*.



41. Consumers were exposed to the misleading representations by both Zelle and Chase that not only were Defendants' services connected and therefore covered by the same protections that consumers had benefitted from for years through Chase, but also that in the event of a fraudulent transaction, Zelle informed customers they were explicitly entitled to getting their money back.

42. Had Defendants properly disclosed the risks associated with using Zelle, and been forthcoming to consumers that the protections of their Chase accounts did not extend to their use of Zelle, consumers would not have believed that any fraud they experienced entitled them to reimbursement by Defendants.

EFTA and Regulation E Require Financial Institutions to Reimburse Consumers for Unauthorized Zelle Transactions

43. In 1978, Congress passed the EFTA, 15 U.S.C. § 1693 *et seq*., which was designed to protect individual consumers engaging in electronic fund transfers. The EFTA lays out definitions, terms, requirements, rights, and limitations for consumers and financial institutions engaging in the electronic sending of money.

44. On July 21, 2011, Title X of the Dodd-Frank Act transferred rulemaking authority of the EFTA from the Board of Governors of the Federal Reserve System to the CFPB, including the

implementation of Regulation E, which "provides a basic framework that establishes the rights, liabilities, and responsibilities of participants in an electronic fund transfer system."[26]

45. According to the CFPB, Regulation E classifies covered transactions as "electronic fund transfer[s] that authorizes a financial institution to debit or credit a consumer's account."[27] It continues, "The term 'electronic fund transfer' or 'EFT' means 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 CFR 1005.3(b)(1). Accordingly, Regulation E applies to any person-to-person (P2P) or mobile payment transaction that meets the definition of an EFT, including debit card, ACH, prepaid account, and other electronic transfers to or from a consumer account.[28]

46. The CFPB Frequently Asked Questions page explains:

> 2. Can person-to person or "P2P" payments be EFTs under Regulation E?
>
> **Yes.**
>
> Person-to-person or "P2P" payments allow a consumer to send money to another person without needing to write a check, swipe a physical card, or exchange cash. Depending on the payment provider, a P2P payment can be initiated from a consumer's online bank account portal, prepaid account portal, or mobile application.[29]

---

[26] https://www.federalreserve.gov/supervisionreg/regecg.htm#:~:text=Regulation%20E%20provides%20a%20basic,preauthorized%20transfers%20from%20or%20to (last accessed Feb. 28, 2023).

[27] 12 CFR § 1005.3(a).

[28] 12 CFR § 1005.3(b)(1)(v); Comment 3(b)(1)-1.ii.

[29] https://www.consumerfinance.gov/compliance/compliance-resources/deposit-accounts-resources/electronic-fund-transfers/electronic-fund-transfers-faqs/#financial-institutions-2 (last accessed Feb 21, 2023) (emphasis added).

47. Regulation E further defines covered "financial institutions" to include "providers of P2P payment and bill payment services, if they directly or indirectly hold an account belonging to a consumer, or if they issue an access device and agree with a consumer to provide EFT services.[30]

48. Regulation E requires all covered financial institutions to investigate any claim of error on a consumer's account and either rectify the error or provide the results of its investigation along with an explanation of the findings as to why the transfer was found to be authorized. The regulation provides that "[a]ny entity that is considered a financial institution under Regulation E has error resolution obligations in the event that a consumer notifies the financial institution of an error, with limited exceptions."[31]

49. Most relevant to Defendant Zelle is the CFPB's example of a non-bank P2P payment provider that is considered a financial institution under Regulation E: "An example of an account that a non-bank P2P payment provider may directly or indirectly hold is a prepaid or mobile account whose primary function is to conduct P2P transfers."[32]

50. Once an entity is classified as a financial institution under Regulation E, the entity becomes liable for error resolution on consumers' accounts. For the purposes of the EFTA and Regulation E, errors include unauthorized EFTs.[33] Proper error resolution requires that once a financial institution has received verbal or written notice of an error from a consumer, the financial institution must: (1) quickly investigate the alleged error, (2) complete its investigation within

---

[30] *Id*.
[31] 12 CFR § 1005.11.
[32] 12 CFR § 1005.3(b)(3); Comment 2(b)(3)(i)-10.
[33] https://www.consumerfinance.gov/compliance/compliance-resources/deposit-accounts-resources/electronic-fund-transfers/electronic-fund-transfers-faqs/#financial-institutions-2 (last accessed Feb. 21, 2023).

Regulation E time limits, (3) report the investigation results within three days of completion, and (4) correct the error within one business day of determining an error did occur on the account.[34]

51. An unauthorized EFT is defined as "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 benefit . . . . 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."[35]

52. Most pertinent to Plaintiff's claims, the CFPB specifically defines fraudulent activity on consumers' P2P accounts as unauthorized EFTs. "Because the EFT was initiated by a person other than the consumer without actual authority to initiate the transfer – *i.e.*, the fraudster – and the consumer received no benefit from the transfer, the EFT is an unauthorized EFT. 12 CFR 1005.2(m). This is true even if the consumer does not have a relationship with, or does not recognize, the non-bank P2P payment provider."[36]

53. Regulation E also prevents financial institutions from contractually waiving their liability through user agreements. The EFTA includes an anti-waiver provision stating that "[n]o writing or other agreement between a consumer and any other person may contain any provision which constitutes a waiver of any right conferred or cause of action created by [EFTA]."[37]

---

[34] *See* 12 CFR § 1005.11(c)(1).
[35] 12 CFR § 1005.3(m); Comments 2(m)-3 and 4.
[36] https://www.consumerfinance.gov/compliance/compliance-resources/deposit-accounts-resources/electronic-fund-transfers/electronic-fund-transfers-faqs/#financial-institutions-2 (last accessed Feb. 21, 2023).
[37] 15 U.S.C. § 1693I.

Chase and Zelle Failed to Reimburse Ms. Glavin for Unauthorized Zelle Transactions

54. From June 6, 2022 to June 8, 2022, Ms. Glavin was traveling with her domestic partner from her home in Pennsylvania on a trip to New Jersey.

55. In the five days following the trip, numerous unauthorized transactions occurred in Ms. Glavin's account, debiting sometimes $2,000 at a time.

56. On June 6, 2022, Ms. Glavin's Chase account was debited via Zelle in the amount of $2,000 to an account name of "Kimberly" with a description of "mining fee."

57. On June 6, 2022, Ms. Glavin's Chase account was debited via Zelle in the amount of $2,000 to an account name of "Erhauyi" with a payment description of "tax."

58. On June 8, 2022, Ms. Glavin's Chase account was debited via Zelle another $2,000 to the same account under the name "Erhauyi" with the payment description of "remainder."

59. On June 9, 2022, Ms. Glavin's Chase account was debited via Zelle $500 to the same "Erhauyi" account with no payment description.

60. These unauthorized Zelle transactions resulted in $6,500 being taken from Plaintiff's checking account with Chase.

61. When Ms. Glavin returned from her trip, she checked her mortgage payment application, which includes a credit check section, at which time she discovered the $6,500 in fraudulent Zelle transactions. Immediately upon discovering the fraudulent Zelle transactions, Ms. Glavin contacted Chase to dispute the transactions. The Chase representative on the phone recommended Ms. Glavin visit her local Chase branch to have an employee file her claims. The next day, June 11, 2022, Ms. Glavin went to her local Chase bank, and a Chase employee collected her documentation and timeline and filed a fraud claim with Chase.

62. On June 11, 2022, Chase sent Ms. Glavin a request for additional information in the form of a Disputed Transaction Questionnaire, which she completed and returned to Chase on the same day.

63. Ms. Glavin initially received a notice from Chase that her account was being temporarily credited the $6,500 that was stolen through the fraudulent Zelle transactions. The notice stated Chase was investigating the transactions Ms. Glavin reported as fraudulent but, if they determined the transactions were authorized or correct, the credit would be reversed.

64. On June 24, 2022, Chase Bank denied Ms. Glavin's claim of fraudulent activity and has since refused to reimburse her for the money taken from her account through the fraudulent Zelle transactions without her permission or authorization. The notice Ms. Glavin received from Chase stated that the claim was denied because the transactions were processed "according to the information you provided or was authorized." The notice informed Ms. Glavin that Chase was removing the $6,500 credit from her account.

65. After the denial, Ms. Glavin submitted a complaint regarding the denial via email to Chase. She submitted additional documentation, including credit card statements and hotel itineraries, proving her location to be outside of where the transactions occurred, as well as a statement from her partner attesting to their location at the time of the fraud.

66. On August 30, 2022, Chase responded to Ms. Glavin's second complaint, informing her that the denial remained "unchanged as we have no new evidence or information to support the claim."

67. Ms. Glavin did not release her Zelle login information to anyone, nor was she the victim of a scam in which fraudulent persons persuade users to send them money.

68. As of the date this Complaint is filed, Chase has failed to reimburse Ms. Glavin for any of the unauthorized, fraudulent Zelle transactions.

Chase and Zelle's Failure to Refund Ms. Glavin's Unauthorized, Fraudulent Transactions Violated EFTA and Regulation E

69. Pursuant to Regulation E, if Defendants receive notice from a consumer in which the consumer enables the financial institution to identify the name and account number of the consumer, indicates the consumer's belief that there was an error on the account, and sets forth reasons for the consumer's belief, Defendants must investigate the allegations and report the results of the investigation to the consumer within 10 business days.

70. Chase received such required notice from Ms. Glavin and, after a cursory investigation, reported the findings of the transactions as "authorized" and provided Ms. Glavin with only a one-sentence explanation that it would be removing the provisional reimbursement because the transactions allegedly were made from Ms. Glavin's phone.

71. Because Ms. Glavin's phone is her access device as defined by Regulation E, and she did not initiate or authorize any of the fraudulent Zelle transactions, any access to her account through her phone is unauthorized under the EFTA. Defendants are therefore liable for the fraudulent Zelle transactions on her account.

72. Regulation E defines errors that must be corrected as **unauthorized electronic transfers**, incorrect electronic fund transfers, computational errors by financial institutions, consumers' receipts of incorrect amounts of money from electronic terminals, omissions from a period statement of an electronic fund transfer that affects the consumer's account which should have been included, and any other error described in the CFPB regulations. 15 U.S.C. § 1693f(f)(1)-(7) (emphasis added).

73. Because Ms. Glavin's account was plagued with unauthorized electronic transfers, Defendants, not Ms. Glavin, are liable for the fraudulent Zelle transactions under Regulation E. Defendants' failure to correct these errors is therefore a violation of EFTA.

74. Because Ms. Glavin followed all of the applicable notice requirements under Regulation E, Defendants are liable for any funds lost because of the unauthorized Zelle transfers, as well as any interest on the stolen funds.

75. Defendants neither corrected the errors on Ms Glavin's account based on the unauthorized transactions, as they are required to do under EFTA and Regulation E, nor did they provide a valid explanation of the determination that the transactions were authorized by Ms. Glavin. Even upon Ms. Glavin supplementing her original fraud claim with documentation establishing that she was not in the geographic location where the transfers originated from at the time they were initiated, Defendants still failed to correct the error and credit Ms. Glavin for the fraudulent transactions..

76. Defendants similarly are required to provide consumers, including Ms. Glavin, with the "identity of any third party to whom or from whom funds are transferred" at the time of an EFT. 15 U.S.C. § 1693d(1)(4). Ms. Glavin has asked for the information identifying where the transfers from her account were sent and has only been provided with the labels on Zelle that contain no identifying information such as "Kimberly" and "Erhauyi." Defendants therefore did not provide the requisite documentation of the transfers to Ms. Glavin.

77. Defendants further did not meet their burden of proof in establishing that the transactions were, in fact, authorized by Ms. Glavin. Regulation E imposes the burden on financial institutions to affirmatively prove that the transactions were authorized. Defendants failed meet this burden and failed to provide an adequate explanation of how they met this burden in either notice provided to Ms. Glavin. Accordingly, Defendants' inadequate and incomplete investigation and conclusory

"explanation" as to why they would not be reimburse Ms. Glavin for the fraudulent Zelle transactions further violates Regulation E.

Defendants Are Well Aware That Zelle Fraud Is Pervasive on Their Platforms

78. Defendants were well-aware of the fact that Zelle fraud was pervasive on their platforms prior to June 6, 2022. Defendants took virtually no precautionary steps to protect consumers, likely because it financially behooves Defendants not to do so.

79. Indeed, the unauthorized, fraudulent transactions that occurred on Ms. Glavin's account are not isolated incidents.

80. Senator Warren's investigation into the rampant fraud on Zelle found that reports of fraud on the Zelle platform are more than twice as high as for comparable banks. Since Defendants integrated Zelle into their banking apps, the frequency of fraud reported on accounts held by Zelle-owned banks is 2.5 times higher now than it was in 2019.

81. In October 2022, CNN described the fraud on the Zelle platform as exploding, and accused the platform and banks of refusing to handle the rampant claims.[38]

82. In November 2022, credit reporting agency Credit Karma published an article warning consumers of the rarity of reimbursement for fraud claims on the Zelle system.[39]

83. As recently as January 2023, NBC reported how popular Zelle is with thieves, and that each year, "millions of dollars are stolen from consumers through Zelle in fraudulent transfers," highlighting that victims rarely receive these stolen funds back from their banks.[40]

---

[38] *Supra* note 4.
[39] https://www.creditkarma.com/news/i/how-to-avoid-zelle-scams (last accessed Feb. 28, 2023).
[40] Lisa Parker and Tom Jones, Zelle Fraud: More People Tricked Into Sending Money Over Popular E-Pay Option, NBC (Jan. 11, 2023 10:36pm) (https://www.nbcchicago.com/consumer/zelle-fraud-more-people-tricked-into-sending-money-over-popular-e-pay-option/3043036/).

84. Moreover, Chase has a perverse financial incentive to never reimburse these unauthorized, fraudulent transactions. If funds are taken from a Chase account by another bank via a fraudulent Zelle transaction, Chase will not receive the money back without the deposited bank agreeing to do so.

85. Because Chase has no financial incentive or possibility of reimbursement itself if it reimburses fraud victims whose accounts are debited by other banks, it typically does not provide reimbursements for these fraudulent transactions in violation of federal law.

V. CLASS ALLEGATIONS

86. Plaintiff brings this action on behalf of herself and on behalf of all other persons similarly situated.

87. Plaintiff is a member of and seeks to represent a nationwide Class, pursuant to Fed. R. Civ. P. 23(b)(2), (b)(3), and/or (b)(4), defined as:

> All persons within the United States whose bank accounts with Chase were debited via an unauthorized transaction using the Zelle mobile application that was not permanently credited by Defendants in full within 45 days of a dispute by the customer or the customer's authorized representative concerning the transaction.

88. Additionally, Plaintiff is a member of and seeks to represent a Pennsylvania Subclass, pursuant to Fed. R. Civ. P. 23(b)(2), (b)(3), and/or (b)(4), defined as:

> All Chase customers in Pennsylvania whose bank accounts with Chase were debited via an unauthorized transaction using the Zelle mobile application that was not permanently credited by Defendants in full within 45 days of a dispute by the customer or the customer's authorized representative concerning the transaction.

89. Excluded from the Class and Subclass are Defendants' officers, directors, and employees; any entity in which Defendants have a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendants. Further excluded from the Class and

Subclass are members of the judiciary to whom this case is assigned, their families, and members of their staff.

90. Plaintiff reserves the right to modify the proposed class definitions, including but not limited to expanding the class to protect additional individuals and to assert additional subclasses as may be warranted by additional investigation.

91. Numerosity: The members of the Class and Subclass are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time, based on information and belief, the Class and Subclass consists of at least thousands of individuals nationwide.

92. Ascertainability: Although the exact number and identities of the Class members are unknown at this time and can only be ascertained through discovery, identification of the Class members is a matter capable of ministerial determination from Defendant's records.

93. Commonality: There are questions of law and fact common to the Class and Subclass, which predominate over any questions affecting only individual Class members. These common questions of law and fact include, without limitation:

a. Whether Plaintiff and the Class and Subclass lost money that was transferred without authorization from their bank account via Zelle;

b. Whether Plaintiff and the Class and Subclass were customers of Chase at the time of the unauthorized transactions;

c. Whether Chase violated the EFTA by failing to adequately investigate the disputes of Plaintiff and the Class and Subclass;

d. Whether Chase violated the EFTA by failing to correct errors on the accounts of Plaintiff and the Class and Subclass;

e. Whether the transactions at issue were unauthorized by EFTs, making them errors subject to the EFTA's remedial provisions;

f. Whether Plaintiff and the Class and Subclass are entitled to maximum statutory damages under the EFTA;

g. Whether Defendants violated Pennsylvania's Unfair Trade Practices and Consumer Protection Law;

h. Whether Defendants were negligent in their actions or omissions; and

i. Whether Plaintiff and the Class and Subclass are entitled to injunctive relief.

94. Typicality: Plaintiff's claims are typical of those of other Class and Subclass members because, like other putative Class and Subclass members, Plaintiff was the victim of fraudulent unauthorized transactions from her Chase account through the Zelle mobile application. After disputing the unauthorized transactions, Plaintiff was informed by Chase that the unauthorized transactions would ultimately not be reversed or reimbursed by the bank.

95. Adequacy of Representation: Plaintiff will fairly and adequately represent and protect the interests of Class and Subclass members. Plaintiff's Counsel are competent and experienced in litigating consumer class actions.

96. Predominance: Defendants have engaged in a common course of conduct toward Plaintiff, Class members, and Subclass members, in that Plaintiff, Class, and Subclass members all had money in their Chase accounts withdrawn through unauthorized transactions on the Zelle payment system. The common issues arising from Defendants' conduct affecting Class and Subclass members set out above predominate over any individual issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

97. Superiority: A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class and Subclass members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class and Subclass members would create a risk of inconsistent or varying adjudications with respect to individual Class and Subclass members, which would establish incompatible standards of conduct for Defendants. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class and Subclass member.

98. Defendants have acted on grounds that apply generally to the Class and Subclass, so that class certification is appropriate.

99. Notice: Plaintiff anticipates providing direct notice to the Class and Subclass for purposes of class certification, via U.S. Mail and/or email, based upon Defendants' and/or Defendants' agents' records.

VI. EQUITABLE RELIEF

100. Absent an equitable injunction enjoining Defendants' conduct alleged herein, Plaintiff and the Class and Subclass members, as well as other Chase and Zelle users, will be irreparably harmed and denied an effective and complete remedy because they face a real and tangible threat of future harm emanating from Defendants' ongoing conduct. Defendants' policy of failing to reimburse customers for unauthorized, fraudulent Zelle transactions cannot be remedied with monetary damages alone.

101. Ms. Glavin continues to hold a checking account with Chase, and Zelle is inextricably linked with her Chase account within the Chase mobile banking platform. If the Court were to enter an injunction requiring Defendants to adequately investigate fraud claims and to reimburse fraudulent EFTs, Plaintiff would want to continue to use her Chase and Zelle accounts. Without an injunction, Plaintiff cannot trust Defendants' security or fraud protection claims and would not continue using their services.

102. Moreover, damages alone would not prevent Defendants from continuing to provide inadequate protection for customers' EFTs and failing to properly investigate such claims about their services, nor from continuing with these deceptive trade practices. No amount of money can rectify the harm caused to future consumers.

VII. FIRST CAUSE OF ACTION

VIOLATION OF THE ELECTRONIC FUND TRANSFER ACT

15 U.S.C. §§ 1693, *ET SEQ.*

(On Behalf of Plaintiff and the Nationwide Class Against All Defendants)

103. Plaintiff realleges and incorporates herein by reference the allegations contained in all preceding paragraphs, and further alleges as follows:

104. EFTA 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).

105. "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. § 1693(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 errors, 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).

106. 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. *Id*.

107. 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) days after receipt of notice of error to investigate. *Id*. § 1693f(c).

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

109. An 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 P2P or mobile payment transaction that meets the definition of EFT. 12 C.F.R. 1005.3(b)(1)(v); *id*., Comment 3(b)(1)-1ii.

110. 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).

111. According to the CFPB, unauthorized EFTs include transfers initiated by a person who obtained a consumer's access device through fraud or robbery.[41]

[41] https://www.consumerfinance.gov/compliance/compliance-resources/deposit-accounts-resources/electronic-fund-transfers/electronic-fund-transfers-

112. 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's account is accessed by a third party by fraudulent means, and the third party uses that information to make an EFT from the consumer's account, the transfer is an unauthorized EFT under Regulation E.[42]

113. Here, Plaintiff and other Class members had their Chase accounts deducted through unauthorized third-party transactions on the Zelle system. The accounts were accessed through hacking or other fraudulent means, and Plaintiff and Class members did not give any third party access to the accounts or permission to deduct funds from them using Zelle.

114. In each case, the third party used the Zelle payment system to fraudulently make unauthorized EFTs from the accounts of Plaintiff and other Class members from their Chase accounts.

115. After the unauthorized EFTs were made, said EFTs appeared on the bank statements of Plaintiff and other Class members.

116. Plaintiff and other Class members notified Chase of these errors within sixty (60) days of their appearances on the accounts of Plaintiff and other Class members.

117. Chase then issued provisional credits in the amounts of those credits on the accounts of Plaintiff and the Class members.[43]

---

faqs/?_gl=1*1negw7n*_ga*MTU2Mzc2MzY0NC4xNjc0Nzc5NTEx*_ga_DBYJL30CHS*MTY3NDc3OTUxMS4xLjEuMTY3NDc4MDAxNC4wLjAuMA.. (last accessed Jan. 26, 2023).

[42] *Id*.

[43] https://www.chase.com/personal/credit-cards/education/basics/provisional-credit (last accessed Feb. 21, 2023).

118. After receiving notice of the unauthorized EFTs on the accounts of Plaintiff, Chase reversed the provisional credits placed on her account and has refused to provide a refund for her unauthorized Zelle transactions.

119. As a direct and proximate result of Defendants' conduct, Plaintiff and other Class members were unable to reclaim funds that were fraudulently taken from their accounts with Chase.

120. Upon information and belief, Chase knowingly and willfully concluded that the transfers of funds via Zelle on accounts of Plaintiff and other Class members 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).

121. Upon information and belief, Chase intentionally determined that the unwanted transfer of funds via Zelle on accounts of Plaintiff and other Class members were not in error due to, at least in part, Chase's financial self-interest as an owner and stakeholder in Zelle.

122. As such, Plaintiff and other Class members 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 Chase; and (iv) reasonable attorneys' fees and costs. *Id*. §§ 1693f(e)(2), 1693m(a)-(b).

VIII. SECOND CAUSE OF ACTION

NEGLIGENCE

(On Behalf of Plaintiff and the Nationwide Class Against All Defendants)

123. Plaintiff realleges and incorporates herein by reference the allegations contained in all preceding paragraphs, and further alleges as follows:

124. Chase owed Plaintiff and the Class at least a duty to take reasonable steps to safeguard customer financial information and protect their financial accounts from malicious third parties,

adequately warn of known risks and/or dangers associated with the Zelle mobile application, and properly investigate disputed transactions accomplished through the Zelle mobile application.

125. Zelle owed Plaintiff and the Class at least a duty to take reasonable steps to adequately warn of known risks and/or dangers associated with the Zelle mobile application, and to take appropriate steps in response to known fraud involving the mobile application to protect consumers from malicious third parties.

126. Defendants breached their obligations to Plaintiff and the Class and were otherwise negligent and/or reckless by at least:

a. Failing to maintain adequate data security measures to prevent or reduce the risk of disclosure of the names, phone numbers, and bank affiliation of Plaintiff and the Class to malicious third parties;

b. Failing to adequately protect the private information of Plaintiff and the Class;

c. Failing to properly warn Plaintiff and the Class of the risks and/or dangers associated with the Zelle mobile application;

d. Failing to take appropriate steps to avoid unauthorized transactions through the Zelle mobile application in response to known scams and continuing with business as normal;

e. Failing to adequately investigate the unauthorized transactions made on the accounts of Plaintiff and the Class using the Zelle mobile application;

f. Failing to implement appropriate and sufficient safeguards against fraud of the nature alleged in the Complaint in light of the knowledge that the fraud has been rampant across the country;

g. Failing to reverse unauthorized transactions following disputes of Plaintiff and the Class despite Defendants' knowledge that such transactions were unauthorized as part of fraud that was well-known to Defendants; and

h. Failing to permanently reverse unauthorized transactions upon a sufficient showing by Plaintiff and the Class that said transactions were unauthorized.

127. As a direct and proximate result of Defendants' breach, Plaintiff and the Class members lost funds from their Chase accounts.

128. Accordingly, on information and belief, Plaintiff and Class members have lost millions of dollars and further face a continuing and increased risk of fraud and loss of money.

IX. THIRD CAUSE OF ACTION

VIOLATION OF PENNSYLVANIA UNFAIR TRADE PRACTICES AND CONSUMER PROTECTION LAW ("UTPCPL") (73 P.S. §§ 201-1 – 201-10)

(On Behalf of the Pennsylvania Subclass Against All Defendants)

129. Plaintiff realleges an incorporates herein by reference the allegations contained in all preceding paragraphs, and further alleges as follows:

130. Defendants are and were at all times relevant "persons" as defined in the UTPCPL. 73 P.S. §201-2(2).

131. Defendants provide and at all times relevant provided "trade" and "commerce" as defined in the UTPCPL as "the advertising, offering for sale, sale or distribution of any services . . . ." 73 P.S. § 201-2(3).

132. The UTPCPL defines "Unfair trade practices" to include any of the following:

a. Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits or quantities that they do not have;

b. Representing that goods or services are of a particular standard, quality or grade, if they are of another;

c. Advertising services with intent not to sell them as advertised; or

d. Failing to comply with the terms of any written guarantee or warranty given to buyer at, prior to or after a contract for the purchase of services is made.

Characteristics Services Do Not Have

133. A service contains characteristics or benefits they do not have under the UTPCPL if they are represented to have such characteristics or benefits but the services actually delivered do not contain said characteristics or benefits.

134. Defendants tout Zelle as being a safe and reliable method of sending money across accounts. The Chase webpage titled "Why Zelle?" claims Zelle is "A fast and easy way to send and receive money to almost anyone you know who has a bank account in the U.S. right in your Chase Mobile app."[44]

135. Chase's web page also indicates the Zelle app and Chase bank are integrated, leading consumers to believe Zelle payments are afforded the same protection as other payments made from their Chase accounts. "The benefits of sending and receiving money are already in the Chase Mobile app, so there is no new app to download or extra steps to take. Just sync your contacts from your mobile phone to make it easy for friends and family to send you money."[45]

136. Defendant Chase's website also contains a bolded header of "**Secure**" under which the website claims "Your account information stays protected. You won't see the other person's bank account info, and they won't see yours."[46]

[44] https://www.chase.com/personal/zelle (last accessed Jan. 31, 2023).
[45] *Id*.
[46] *Id*.

137. Defendants' actions constitute a representation of characteristics or benefits of the Zelle services that the services do not actually have because, as alleged above, they intentionally lead consumers to believe the Zelle app was synonymous with the Chase banking platform and was therefore afforded the same fraud protections under federal law.

138. Defendants knew the Zelle platform was not as secure as Chase's other methods of payments and did not take adequate measures to inform consumers that the Zelle application did not contain the same characteristics and benefits the rest of Chase banking offers.

139. Defendants' conduct was likely to and did in fact lead Plaintiff and the Subclass members to believe that the Zelle payment system contained the characteristics and benefits of the Chase banking services, when, in reality, it does not. This is therefore a violation of the UTPCPL. 73 P.S. § 201-2(4)(v).

Services of a Particular Standard

140. A service is violative of the UTPCPL if it is represented to be of a particular standard but is, in fact, of another. 73 P.S. §201-2(4)(vii).

141. Defendants' actions constitute a representation of the Zelle payment service as a particular standard of safe and secure, when, in fact, it is not.

142. As alleged above, Defendant Chase's website claims the Zelle payment system is secure and safe, even implying that it is safer than the use of paper checks since the other users will not have access to the user's account number as they would on a physical check.

143. However, Defendants were aware of the risk of fraud on the Zelle platform and continued to represent the service was of a higher standard of security.

144. Even in spite of the open letter from U.S. senators highlighting the deficiencies in the service, Defendants continue to represent that Zelle is of a high security standard.

Advertising Services with Intent Not to Sell as Advertised

145. Under the UTPCPL, a violation occurs when a service is advertised when the provider does not intend to provide the service as advertised. 73 P.S. § 201-2(4)(ix).

146. Defendants' actions constitute an advertisement of services with intent not to sell the services as advertised because, as alleged above, Defendants advertised a safe and secure payment transfer method, with indications that the service would be provided with the protections afforded by the banks that own Zelle.

147. The aforementioned claims by Defendant Chase on its website regarding the security of the Zelle payment system, along with the implications that Zelle was synonymous with Chase as it was already built into the Chase banking mobile application, all constitute advertisements to provide Zelle in a manner that differed from what was actually provided.

148. Because Defendants advertised Zelle services with the intent not to provide the services as advertised, Defendants are liable to Plaintiff and the Subclass members for violation of the UTPCPL.

Breach of Warranty

149. Pursuant to the UTPCPL, "failing to comply with the terms of any written guarantee or warranty given to the buyer at, prior to or after a contract for the purchase of goods or services is made" is a violation of the law. 73 P.S. § 201-2(4)(xiv).

150. Defendants' conduct constitutes a failure to comply with the terms of a written guarantee because of the statements from Defendant Chase regarding Zelle's secure payment system alleged above.

151. Defendants in writing informed consumers the Zelle platform was secure, despite their intent to deny claims of unauthorized use made via fraud on the platform.

152. Defendants represented to consumers that Zelle was backed by the banks that own it, and therefore made guarantees that consumers have come to expect when fraud occurs in their accounts. Defendants, however, breached this warranty to consumers by failing to reimburse Plaintiff and the Subclass members who suffered financial losses due to the Zelle fraud.

153. All conduct by Defendants which does not provide the protections of Chase accounts, and which fails to provide a safe and secure payment system, which consumers were promised in writing, therefore constitutes a failure to comply with the terms of a written guarantee.

154. Because Defendants failed to comply with the written terms of the guarantee to consumers regarding the security of the Zelle payment system, Defendants are liable to Plaintiff and the Subclass for violations of the UTPCPL. 73 P.S. § 201-2(4)(xiv).

155. These acts and practices alleged were intended to or did result in violations of the UTPCPL.

156. Chase has and will continue to unlawfully deny transaction disputes of Plaintiff, the Subclass, and the public by claiming that such transactions are actually "authorized" transactions, even though said transactions are actually "unauthorized," as the term is defined by EFTA and applicable regulations. Consequently, the practices of Chase constitute unfair or deceptive trade practices within the meaning of the UTPCPL.

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

X. PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for relief and judgment against Defendants, and each of them, as follows:

a. Class certification of this action;

b. Appointment of Plaintiff as Class representative;

c. Appointment of Plaintiff's attorneys as Class Counsel;

d. An award of actual damages, in an amount to be determined at trial;

e. An award of treble damages against Chase pursuant to the EFTA;

f. An award of the lesser of $500,000.00 or one percent (1%) of the net worth of Chase;

g. Injunctive and other equitable relief against Defendants as necessary to protect the interests of Plaintiff and other Class members, and an order prohibiting Defendants from engaging in unlawful and/or unfair acts described above, including public injunctive relief;

h. An order of restitution from Defendants;

i. An order declaring Defendants' conduct as unlawful;

j. Costs of suit;

k. Pre- and post-judgment interest;

l. An award of reasonable attorneys' fees; and

m. Any other relief the Court may deem just and proper, including interest.

XI. DEMAND FOR TRIAL BY JURY

Plaintiff, individually, and on behalf of all others similarly situated, hereby demands a jury trial on all claims so triable.

Dated: May 4, 2023

Respectfully submitted,

MILLER SHAH LLP

/s/ James C. Shah
James C. Shah (Bar No. 80337)
jcshah@millershah.com
Alec J. Berin (Bar No. 328071)
ajberin@millershah.com
1845 Walnut Street, Suite 806
Philadelphia, Pennsylvania 19103
Telephone: (866) 540-5505
Facsimile: (866) 300-7367

SCHUBERT JONCKHEER & KOLBE LLP

Robert C. Schubert (*pro hac vice to be filed)*
rschubert@sjk.law
Amber L. Schubert (*pro hac vice to be filed)*
aschubert@sjk.law
Lila M. Garlinghouse (*pro hac vice to be filed)*
lgarlinghouse@sjk.law
2001 Union Street, Suite 200
San Francisco, California 94123
Telephone: (415) 788-4220
Facsimile: (415) 788-0161

Attorneys for Plaintiff Glavin and the Putative Class

ClassAction.org
