1052753142

CJ22 5078-
Stinson

IN THE DISTRICT COURT OF OKLAHOMA COUNTY
STATE OF OKLAHOMA

SHAKIRA STAFFORD, on behalf of herself and all others similarly situated,

Plaintiff,

v.

TINKER FEDERAL CREDIT UNION
-and-
UNKNOWN MERCHANT PAYMENT PROCESSOR

Defendants.

Case No.: CJ-2022-5078

CLASS ACTION PETITION

JURY TRIAL DEMANDED

FILED IN DISTRICT COURT
OKLAHOMA COUNTY

OCT 14 2022

RICK WARREN
COURT CLERK

50

Plaintiff, SHAKIRA STAFFORD ("Stafford" or "Plaintiff"), by and through her attorneys, brings this Class Action Petition against the Defendants, TINKER FEDERAL CREDIT UNION ("TFCU") and UNKNOWN MERCHANT PAYMENT PROCESSOR, alleging as follows:

INTRODUCTION

1. This is a civil action seeking monetary damages, and injunctive and declaratory relief, from the Defendant(s), TFCU, the largest credit union in Oklahoma, and a merchant payment processing agent, Unknown Merchant Payment Processor ("UMPP"), arising from their collective failure to safeguard the highly sensitive customer data, including credit and debit card numbers as well as cardholder names, account numbers, expiration dates, card verification values ("'CVV"), and PIN data for debit cards (collectively, Payment Card Data, "PCD") of *scores* of TFCU's customers, including Plaintiff Stafford and the proposed Class Members, resulting in a data breach on or about August of 2022 in which the PCD was compromised and unauthorizedly disclosed to and accessed by cybercriminals, causing widespread injury and monetary damages.

EXHIBIT 1

2. On information and belief, on or about August of 2022 cybercriminals were able to infiltrate UMPP's and/or TFCU's systems and obtain the PCD of TFCU's customers, including Stafford and the proposed Class Members (the "Data Breach").

3. The Data Breach was caused by Defendants' acts and omissions in failing to properly protect Stafford's and the proposed Class Members' PCD.

4. Following the devastating Data Breach, on or about August 18, 2022 TFCU represented that its fraud detection systems were "identifying an unusually high number of debit card fraud attempts..."[1] to customers, but that the Data Breach was not the result of a breach to *its* systems, but possibly a breach to UMPP's systems, whom it failed to identify. It is unknown how many customers were affected in the Data Breach, but Plaintiff believes that the number could exceed 445,000.

5. Stafford is a TFCU customer and Data Breach victim, and she brings this class action on behalf herself and all victims harmed by TFCU's and UMPP's tortious misconduct.

PARTIES

6. Plaintiff, Stafford, is an Oklahoma citizen residing in Shawnee, Oklahoma, in Pottawatomie County, where she intends to remain. Stafford is a Data Breach victim, as she has confirmed via TFCU's toll-free telephone number, and as evident from the facts, as follow below.

7. Defendant, TFCU, is a federal credit union in the State of Oklahoma with a principal address in Oklahoma County at 715 Metropolitan Avenue, Oklahoma City, Oklahoma 73108.

8. On information and belief, Unknown Merchant Payment Processor ("UMPP") is an unknown merchant payment processor whose identity is known solely to TFCU, and who

[1] Facebook, Tinker Federal Credit Union, August 18, 2022 post, available at https://www.facebook.com/TinkerFCU (attached as Exhibit 1).

processes credit and debit card payments for payments for goods and services, including for TFCU customers, Stafford and the members of the proposed Class.

JURISDICTION & VENUE

9. This Court has general *in personam* jurisdiction over the Defendants herein under Okla. Stat. tit. 12 § 2004(F), which permits jurisdiction on any basis consistent with the Oklahoma Constitution and the Constitution of the United States, because Defendant TFCU's principal place of business is located in Oklahoma, it is at home in Oklahoma.

10. This Court has subject matter jurisdiction under Okla. Const. Art. VII, § 7, which gives the Court unlimited original jurisdiction of all justiciable matters, including the matters alleged in this Petition.

11. Venue is proper in this Court under Okla. Stat. tit. 12 §§ 134, 137, 139, 141, 187 because venue is proper herein as to the resident Defendant, TFCU.

BACKGROUND FACTS

A. Defendant TFCU

12. TFCU is a federal credit union based in Oklahoma City, Oklahoma, holding itself out as "the largest credit union in Oklahoma, with over 445,000 members and more than $6 billion in assets," "a not-for-profit, member-owned financial cooperative,"[2] which provides banking services including credit and debit cards, and electronic banking services, including "Home Branch online and mobile banking (Internet account access), Bill Pay, Command Center (telephone audio response), ATMs."[3]

13. Upon information and belief, TCFU operates at least thirty-two (32) locations

[2] Tinker Federal Credit Union website, "About Us," https://www.tinkerfcu.org/membership/about-tfcu/ (last accessed August 24, 2022).
[3] *Id.*

throughout Oklahoma, in Ada, Oklahoma at 1620 Lonnie Abbott Boulevard; Bethany, Oklahoma at 6750 NW 39th Expressway, Bethany, OK; Choctaw, Oklahoma at 2183 N Harper, Choctaw, OK; Crooked Oak campus; Edmond East, Oklahoma at 3141 S Bryant Ave, Edmond, OK; Edmond West, at 1401 N Kelly Avenue, Edmond, OK; Enid, Oklahoma at 801 S Oakwood Rd, Enid, OK; at John Marshall High School; Midwest City, Oklahoma at 6501 Tinker Diagonal, Midwest City, OK; Midwest City East at 1401 S Post Rd, Midwest City, OK; Moore, Oklahoma at 400 SW 6th St, Moore, OK; Norman Southeast, 1451 12th Ave SE, Norman, OK; Norman West, 301 36th Ave NW, Norman, OK; Oklahoma City, Oklahoma, Capitol Hill at 2315 S Western Ave, Oklahoma City, OK; Oklahoma City, Metro Tech, 1800 Springlake Drive, Ste 200, Oklahoma City, OK; Oklahoma City, North Rockwell, 13300 N Rockwell Ave, Oklahoma City, OK; Oklahoma City, Northeast, 1177 NE 23rd St, Oklahoma City, OK; Oklahoma City, Northwest, 4626 NW 39th St, Oklahoma City, OK; Oklahoma City, South Sooner Road at 14900 S Sooner Rd, Oklahoma City, OK; Oklahoma City, Southwest, 9601 S Pennsylvania Ave, Oklahoma City, OK; Oklahoma City, Southwest Drive-Thru, 1200 SW 89th St, Oklahoma City, OK; Oklahoma City, Tri-City, 4101 SW 134th St, Oklahoma City, OK; Seminole, Oklahoma at 2221 N Milt Phillips Ave, Seminole, OK; Shawnee, Oklahoma at 3923 N Harrison Street, Shawnee, OK; Stillwater, Oklahoma at 5101 W 6th Ave, Stillwater, OK; Tinker AFB; Vance Air Force Base, 234 Fields St, Vance AFB, OK; and in Yukon, Oklahoma at 11209 W Reno Ave, Yukon, OK.[4]

14. TFCU promises customers that it will, "[p]rovide the best financial services and convenience for our members using sound financial principles [;] [e]ducate [its] members to better understand and manage their individual financial needs [;] [a]lways do the right thing for our individual members and [its] collective Membership [and to] [a]lways be ethical, honest and

[4] Tinker Federal Credit Union Website, "Locations," available at https://www.tinkerfcu.org/locations/ (last accessed September 28, 2022)

trustworthy."[5]

15. TFCU creates and stores financial account information and PCD for its customers, including credit and debit card information, for Stafford and the proposed Class Members. Further, this PCD includes cardholder names, account numbers, expiration dates, CVVs, and PIN data for debit cards.

16. In offering these services, TFCU acknowledges the risks posed by identity theft of PCD, educating its customers that, "identity theft is a crime where a thief steals your personal information, such as your full name or Social Security Number, to commit fraud," and that, "[w]ith this information, the thief can fraudulently apply for credit, file taxes or get medical services. These acts can damage your credit status and cost you time and money to restore your good credit history."[6]

17. Despite recognizing the risk of identity theft that can result from stolen PCD, and despite its duties to protect that information, TFCU does not follow industry standard practices in securing that information and fails to adequately train its employees on cybersecurity policies, enforce those policies, or maintain reasonable security practices and systems.

B. Defendant UMPP

18. On information and belief, UMPP is an unknown merchant payment processor who processes financial transactions including debit card transactions for TFCU customers, including for Stafford and the members of the proposed Class.

19. When TFCU customers pay using credit or debit cards, UMPP receives PCD,

---

[5] Tinker Federal Credit Union Website, "About Us," https://www.tinkerfcu.org/membership/about-tfcu/ (last accessed August 24, 2022).

[6] "Save yourself the risk of becoming an identity theft victim" available at https://www.tinkerfcu.org/save-yourself-the-risk-of-becoming-an-identity-theft-victim/ (last accessed August 24, 2022).

including not only the credit and debit card information but also cardholder names, account numbers, expiration dates, CVVs, and PIN data for debit cards which it utilized to process and complete the payment.

20. UMPP utilizes and stores this PCD, including credit and debit card numbers, for Stafford and the proposed Class Members, within its computer systems, to facilitate its processing of payments for goods and services by Stafford and the members of the proposed Class.

21. According to TFCU, upon information and belief, UMPP "processed transactions from many financial institutions' debit cards in the past..."[7]

22. On or about August 17, 2022, according to TFCU, UMPP's systems were breached, "opening individual [TCFU] debit cards to vulnerability."[8]

23. The Data Breach resulted in the unauthorized disclosure of the PCD of Stafford and the proposed Class Members, causing injury and monetary damages.

24. Despite recognizing the risk of identity theft due to stolen PCD and other personal information, and despite its duties to protect that information, upon information and belief, UMPP does not follow industry standard practices in securing that information and fails to adequately train its employees on cybersecurity policies, enforce those policies, or maintain reasonable security practices and systems.

25. On information and belief, TFCU knew of UMPP's deficient security practices, and nevertheless, by acts of commission or omission, permitted UMPP to process credit and debit card financial transactions of TFCU customers, including Stafford and the proposed Class members, using their PCD.

C. TFCU and UMPP Failed to Safeguard Plaintiff's and Class Members' PCD

[7] Facebook, Tinker Federal Credit Union, available at https://www.facebook.com/TinkerFCU (Exhibit 1) (last accessed October 10, 2022)
[8] *Id.*

EXHIBIT 1

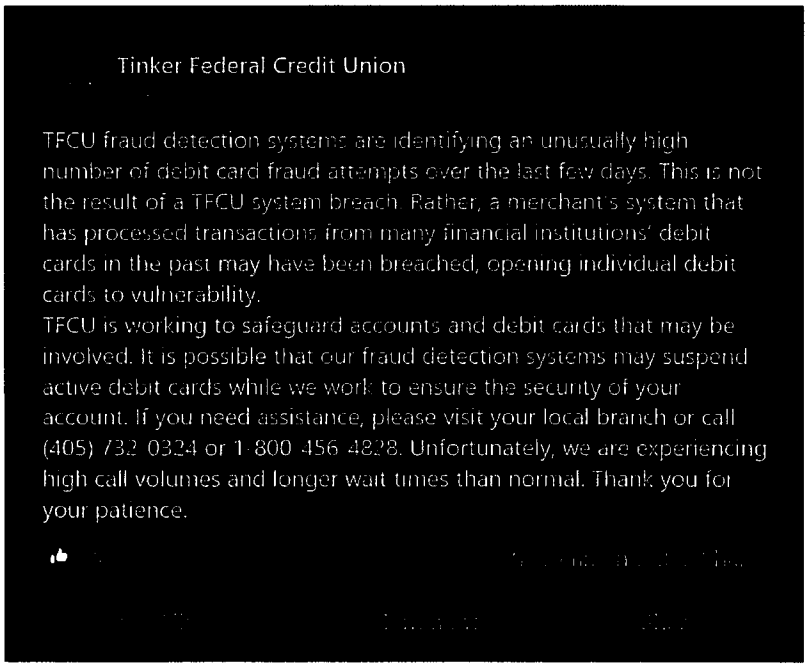
26. On information and belief, as stated above, as a material condition of banking with TCFU and utilizing its credit and debit card services, TFCU creates and electronically stores PCD of its customers on its computer systems, including the card numbers themselves.

27. On information and belief, as stated above, UMPP utilizes TFCU's customers' PCD to process financial transactions for the sale and purchase of goods, and electronically stores the PCD on its computer systems.

28. As described above, TFCU's and/or UMPP's data security safeguards are inadequate to protect the vast amounts of PCD created, stored, and utilized.

29. As a direct and proximate result, on or about August 17, 2022, the PCD of Stafford and the members of the proposed Class stored in UMPP's and/or TFCU's computer systems was unauthorizedly accessed by and disclosed to third party cybercriminals whose sole purpose was the imminent fraudulent and criminal misuse of that PCD.

30. On information and belief, on August 18, 2022 TFCU discovered the Data Breach. On August 18, 2022, at 2:58 p.m., TFCU posted a notice on its social media Facebook page that:


Tinker Federal Credit Union

TFCU fraud detection systems are identifying an unusually high number of debit card fraud attempts over the last few days. This is not the result of a TFCU system breach. Rather, a merchant's system that has processed transactions from many financial institutions' debit cards in the past may have been breached, opening individual debit cards to vulnerability.

TFCU is working to safeguard accounts and debit cards that may be involved. It is possible that our fraud detection systems may suspend active debit cards while we work to ensure the security of your account. If you need assistance, please visit your local branch or call (405) 732 0324 or 1-800 456 4828. Unfortunately, we are experiencing high call volumes and longer wait times than normal. Thank you for your patience.

EXHIBIT 1

See Exhibit 1.

31. Further, TFCU *briefly* posted a notification of the Data Breach on its website, but removed the same shortly thereafter.

32. After discovering the Data Breach, TFCU claims via its Facebook post that it worked to "safeguard accounts and debit cards that may be involved." It is not known what, if any, steps TFCU undertook to protect the PCD unauthorizedly accessed in the Data Breach.

33. TFCU's efforts were inadequate as TFCU was unable to stop cybercriminals from accessing and stealing the PCD of Stafford and the proposed Class Members, as described hereinafter.

34. It is unknown what, if any, investigations TFCU has undertaken to ascertain the identity of UMPP.

35. Regardless, TFCU has failed to disclose the identity of UMPP to customers whose PCD was affected, *to wit,* Stafford and the members of the proposed Class, preventing them from taking reasonable and necessary steps to protect their sensitive PCD from fraudulent misuse, as had now occurred.

36. TFCU notified affected customers via the August 18, 2022 Facebook post, Exhibit 1; by text message to Stafford for fraudulent activity; and notified its employees of the Data Breach by email. TFCU has *not* notified affected customers including Stafford and the proposed Class Members by commonly accepted means, such as U.S. Mail or email, and the Facebook notification will reach only TFCU customers who subscribed to Facebook. Likewise, TFCU has taken down its short-lived notice on their website.

37. In other words, TFCU is obfuscating the nature of the Data Breach, whether to UMPP's systems or to its own, and obfuscated the threat it poses to Data Breach victims.

38. The measures undertaken by TFCU to "safeguard accounts and debit cards that may be involved" should have been in place *before* the breach to its and/or UMPP's systems, evidencing the inadequacy of the affected systems.

39. UMPP has failed to identify itself and notify affected customers of the Data Breach, including Stafford and the members of the proposed Class; and, upon information and belief, has failed to conduct any investigation or take any steps to secure the PCD of Stafford and the proposed Class Members.

40. In other words, UMPP is obfuscating the existence and nature of the Data Breach and the threat it poses to Data Breach victims.

D. Plaintiff's Experience

41. Stafford is a customer and member of TFCU, holding a bank account with said Defendant, and she was issued a debit card by TFCU with a unique debit card number, PCD.

42. Upon information and belief, UMPP received the TFCU PCD of Stafford to process payments for goods and services to merchants.

43. Stafford's PCD was unauthorizedly disclosed in the Data Breach to UMPP's and/or TCFU's computer systems.

44. On or about August 17, 2022, Stafford's PCD was utilized by unknown cybercriminals to make a fraudulent purchase in the sum of $40.00 at "ARA Wayne State."

45. Stafford then received a text message notification from TFCU notifying her of the above fraudulent purchase of $40.00.

46. That same day, TFCU informed Stafford via text message that her debit card had been "locked."

47. Thereafter, Stafford was forced to obtain a new debit card from TFCU, requiring

her to miss work.

48. Further, attendant with the Data Breach permitted to occur by Defendants, Stafford's account with PayPal, linked to her TCFU debit card, was accessed, resulting in further disclosure of PCD and requiring Stafford to change the password on her PayPal account.

49. At all relevant times, UMPP and/or TCFU knew, or reasonably should have known, of the importance of safeguarding customer PCD and the foreseeable consequences that would occur if their data security system(s) were breached, including, specifically, the significant costs that would be imposed on its customers, including Stafford and the members of the proposed Class, as a result of a breach.

50. TCFU was or should have been fully aware of the significant volume of daily credit and debit card transactions processed by UMPP using the PCD, amounting to numerous daily payment card transactions, and thus, the significant number of individuals who would be harmed by a breach of its systems.

51. Unfortunately, despite all this publicly available knowledge of the continued compromises of PCD in the hands of other third parties, such as retailers and merchants, Defendants' approach to maintaining the privacy and security of the PCD of Stafford and the Class members was lackadaisical, cavalier, reckless, or at the very least, negligent.

52. As a direct and proximate result of the Data Breach permitted to occur by Defendant(s), Stafford has incurred monetary damages, and has spent considerable time and effort to remedy the effects of the Data Breach and prevent further injury, and to monitor her accounts to protect herself from identity theft. Stafford fears for her personal financial security and uncertainty over what financial information, PCD, was revealed in the Data Breach. She is experiencing feelings of anxiety, sleep disruption, stress, and fear because of the Data Breach. This

goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that is contemplated and addressed by law.

E. Stafford and the Proposed Class Have Suffered Injury and Damages.

53. Stafford and members of the proposed Class have suffered injury from the misuse of their PCD that can be directly traced to the Data Breach to UMPP's and/or TFCU's systems, occurring because of Defendants' collective acts or omissions.

54. The ramifications of Defendant(s)' collective failure to keep Plaintiff's and the Class's PCD secure are severe. Identity theft occurs when someone uses another's personal and financial information such as her debit card or other information, without permission, to commit fraud or other crimes.

55. As a result of UMPP and/or TFCU failing to prevent the Data Breach, Stafford and the proposed Class have suffered, and will continue to suffer injury and damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered, or are at an increased risk of suffering:

a. theft of their personal and financial information;

b. unauthorized charges on their debit and/or credit card accounts;

c. lost benefits, including PTO time;

d. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

e. damages arising from the inability to use their debit or credit card accounts because their accounts were suspended or otherwise rendered unusable as a result of fraudulent charges stemming from the Data Breach;

f. loss of use of and access to their account funds and costs associated with

inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit including decreased credit scores and adverse credit notations;

g. costs associated with time spent and the loss of productivity or the enjoyment of one's life from taking time to address and attempt to ameliorate, mitigate and deal with the actual and future consequences of the Data Breach. including finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised accounts, and the stress, nuisance and annoyance of dealing with all issues resulting from the Data Breach;

h. the imminent impending injury flowing from potential fraud and identify theft posed by their PCD being placed in the hands of criminals and already misused via the sale of Plaintiffs' and Class members' information on the Internet black market;

i. damages to and diminution in value of their PCD;

j. the loss of Plaintiffs and Class members' privacy; and

k. the continued risk to their PCD which remains in the possession of TFCU and UMPP and is subject to further breaches so long as Defendants fail to undertake the appropriate measures to protect the PCD in their possession.

56. At all relevant times, UMPP and TCFU were each well-aware, or reasonably should have been aware, that PCD collected, maintained and stored in their computer systems is highly sensitive, susceptible to attack, and could be used for wrongful purposes by third parties, such as identity theft and fraud.

57. Indeed, TFCU failed to prevent another cyberattack purloining PCD in 2013.[9]

58. It is well known and the subject of many media reports that PCD is highly coveted and a frequent target of hackers. Despite the frequent public announcements of data breaches with merchants, Defendants maintained an insufficient and inadequate system to protect the PCD of Plaintiff and the Class Members.

59. PCD is a valuable commodity because it contains not only payment card numbers but Personally Identifiable Information ("PII"[10]) as well. A "cyber blackmarket" exists in which criminals openly post stolen payment card numbers, social security numbers, and other personal information on multiple underground Internet websites. PCD is valuable to identity thieves because they can use victims' personal data to open new financial accounts and take out loans in another person's name, incur charges on existing accounts, or clone ATM, debit, or credit cards.

60. Legitimate organizations and the criminal underground alike recognize the value of PII contained in a merchant's data systems; otherwise, they would not seek or pay for it.

61. The value of Plaintiff's and the proposed Class's PCD and/or PII on the black market is considerable. Stolen PII trades on the black market for years, and criminals often post stolen private information openly on various "dark web" internet websites making the information publicly available, for a fee.

---

[9] "TFCU warns customers of security breach" available at https://kfor.com/news/thousand-of-tfcu-customers-at-risk-after-security-breach/ (last accessed August 25, 2022).

[10] The Federal Trade Commission defines "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." 17 C.F.R. § 248.201(b)(8). To be clear, Plaintiff is not suggesting all those varieties of information were necessarily compromised in the Data Breach. However, TFCU failed to apprise class members of exactly what was compromised in the Data Breach, so any of that PII could have been compromised.

62. It can take victims years to spot identity or PII theft, giving criminals time to sell that information for cash.

63. One such example of criminals using PII and PHI for profit is the development of "Fullz" packages.

64. Cybercriminals can cross-reference multiple sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

65. The development of "Fullz" packages means that stolen PII from the Data Breach can easily be used to link and identify it to Plaintiff's and the proposed Class's phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII stolen by the cybercriminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff's and other members of the proposed Class's stolen PII is being misused, and that such misuse is fairly traceable to the Data Breach.

66. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses that year, leading to more than $3.5 billion in losses to individuals and business victims.[11]

67. Further, according to the same report, "rapid reporting can help law enforcement

[11] *See* the FBI's IC3 2019 Internet Crime Report, https://www.ic3.gov/Media/PDF/AnnualReport/2019_IC3Report.pdf (last visited Mar. 23, 2022).

stop fraudulent transactions before a victim loses the money for good."

68. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

69. Along with out-of-pocket expenses that can exceed thousands of dollars for the victim of new account identity theft, and the emotional toll identity theft can take, some victims must spend a considerable time repairing the damage caused by the theft of their PII. Victims of new account identity theft will likely have to spend time correcting fraudulent information in their credit reports and continually monitoring their reports for future inaccuracies, close existing bank/credit accounts, open new ones, and dispute charges with creditors.

70. Further complicating the issues faced by victims of identity theft, data thieves may wait years before trying to use the stolen PII. To protect themselves, Stafford and the Class will need to remain vigilant against unauthorized data use for years or even decades to come.

71. The Federal Trade Commission ("FTC") has also recognized that consumer data is a new and valuable form of currency. In an FTC roundtable presentation, former Commissioner, Pamela Jones Harbour, stated that "most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency."

72. The FTC has also issued several guidelines for both businesses and financial institutions that highlight reasonable data security practices. The FTC has noted the need to factor data security into all business decision-making. According to the FTC, data security requires: (1) encrypting information stored on computer networks; (2) retaining payment card information only as long as necessary; (3) properly disposing of personal information that is no longer needed; (4)

limiting administrative access to business systems; (5) using industry-tested and accepted methods for securing data; (6) monitoring activity on networks to uncover unapproved activity; (7) verifying that privacy and security features function properly; (8) testing for common vulnerabilities; and (9) updating and patching third-party software.

73. According to the FTC, unauthorized PII disclosures are extremely damaging to consumers' finances, credit history, and reputation, and can take time, money, and patience to resolve the fallout. The FTC treats the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5(a) of the FTC Act.

CLASS ACTION ALLEGATIONS

74. Plaintiff Stafford sues on behalf of herself and the proposed Class ("Class"), defined as follows:

> All citizens of the State of Oklahoma whose PCD was compromised in the Data Breach disclosed by TFCU in August 2022.

75. Excluded from the Class are Defendants, their agents, affiliates, parents, subsidiaries, any entity in which Defendants have a controlling interest, any Defendant officer or director, any successor or assign, and any Judge who adjudicates this case, including their staff and immediate family.

76. Plaintiff reserves the right to amend the Class definition.

77. This action satisfies the numerosity, commonality, typicality, and adequacy requirements under Okla. Stat. tit. 12, § 2023.

a. **Numerosity**. Plaintiff is representative of the proposed Class, consisting of thousands of members, far too many to join in a single action;

b. **Typicality**. Plaintiff's claims are typical of Class member's claims as each

arises from the same Data Breach, the same alleged violations by Defendant(s), and the same unreasonable manner of notifying individuals about the Data Breach.

c. **Adequacy**. Plaintiff will fairly and adequately protect the proposed Class's interests. Her interests do not conflict with Class members' interests and she has retained counsel experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf, including as lead counsel.

d. **Commonality**. Plaintiff's and the Class's claims raise predominantly common factual and legal questions that a class wide proceeding can answer for all Class members. Indeed, it will be necessary to answer the following questions:

i. Whether the Data Breach was caused to UMPP's or to TFCU's systems;

ii. Whether Defendants had a duty to protect PCD;

iii. Whether TFCU knew or should have known of the susceptibility of UMPP's systems to a data breach; and whether UMPP knew or should have known of the susceptibility of its systems to a data breach;

iv. Whether Defendants' security measures to protect their POS systems were reasonable in light of FTC data security recommendations, and best practices recommended by data security experts;

v. Whether UMPP and/or TCFU were negligent in failing to implement reasonable and adequate security procedures and practices to safeguard PCD;

vi. Whether UMPP's and/or TCFU's failures to implement adequate data security measures allowed the breach of its systems to occur;

vii. Whether Defendants' acts or omissions constituted unfair or deceptive trade practices;

viii. Whether Defendants' conduct, including their failures to act, resulted in or was the proximate cause of the breach of its systems, resulting in the loss of the PCD of Stafford and Class members;

ix. Whether Plaintiffs and Class members were injured and suffered damages or other acceptable losses because of Defendants' failures to reasonably protect their systems and data network; and,

x. Whether Plaintiffs and Class members are entitled to relief.

78. Further, common questions of law and fact predominate over any individualized questions, and a class action is superior to individual litigation or any other available method to fairly and efficiently adjudicate the controversy. The damages available to individuals are insufficient to make individual lawsuits economically feasible.

COUNT I
Negligence
(On Behalf of Plaintiff and the Class)

79. Plaintiff realleges all previous paragraphs as if fully set forth below.

80. Upon creating, accepting, and storing the PCD of Plaintiff and Class members in their computer systems and on its networks, TFCU and/or UMPP undertook and owed a duty to Plaintiff and the Class members to exercise reasonable care to secure and safeguard that information and to use commercially reasonable methods to do so. Defendants knew that the PCD was private and confidential and should be protected as private and confidential to prevent

imminent injury.

81. TFCU and/or UMPP each owed a duty of care not to subject Plaintiff and Class members, along with their PCD, to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices.

82. TFCU and/or UMPP owed numerous duties to Plaintiff and to members of the Class, including the following:

a. to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting PCD in their possession;

b. to protect PCD using reasonable and adequate security procedures and systems that are compliant with industry-standard practices; and

c. to implement processes to quickly detect a data breach and to timely act on warnings about data breaches.

83. TFCU and UMPP each owed the duty to Plaintiff and the Class members to exercise reasonable care in allowing UMPP to possess its customers PCD and to secure and safeguard that information.

84. TFCU and/or UMPP breached the duties owed to Plaintiff and the Class members to adequately protect and safeguard PCD by knowingly disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured PCD. Furthering their dilatory practices, TFCU failed to provide adequate supervision and oversight of the PCD with which they were and are entrusted, despite the known risk and foreseeable likelihood of breach and misuse, which permitted an unknown third party to gather PCD of Plaintiff and Class members, misuse the Customer Data and intentionally disclose it to others without consent.

85. TFCU and/or UMPP each knew, or should have known, of the risks inherent in collecting and storing PCD, the vulnerabilities of their inadequate systems, and the importance of adequate security.

86. Defendants each knew about numerous, well-publicized data breaches within the banking industry, including one such breach to TFCU's systems in 2013.

87. TFCU and/or UMPP each knew, or should have known, that their data systems and networks did not adequately safeguard Plaintiff's and Class members' PCD.

88. TFCU and/or UMPP each breached their duties to Plaintiff and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard PCD of Plaintiff and Class members.

89. Because Defendants knew that a breach of their systems would damage thousands of TCFU customers, including Plaintiff and Class members, TFCU and/or UMPP had a duty to adequately protect their data systems and the PCD contained therein.

90. TCFU had a special relationship with Plaintiff and the Class members. Plaintiff and Class members' willingness to entrust TCFU with their PCD was predicated on the understanding that TCFU would take adequate security precautions. Moreover, only TCFU had the ability to protect its systems and the PCD it stored on them from attack.

91. UMPP had a special relationship with Plaintiff and the Class members by accepting their PCD. Plaintiff and Class members' willingness to entrust UMPP with their PCD was predicated on the understanding that UMPP would take adequate security precautions. Moreover, only UPMM had the ability to protect its systems and the PCD it stored on them from attack.

92. TFCU's and/or UMPP's own conduct also created a foreseeable risk of harm to Plaintiff and Class members and their PCD, including failing to: (1) secure their systems, despite

knowing their vulnerabilities, (2) comply with industry standard security practices, (3) implement adequate system and event monitoring, and (4) implement the systems, policies, and procedures necessary to prevent this type of data breach.

93. TFCU and/or UMPP also had independent duties under state and federal laws, including the FTC Act and the Gramm-Leach-Bliley Act, that required them to reasonably safeguard Plaintiff's and Class members' PCD and promptly notify them about the Data Breach.

94. TFCU and/or UMPP breached their duties to Plaintiff and the Class members in numerous ways, including:

a. by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard PCD of Plaintiff and Class members;

b. by creating a foreseeable risk of harm through the misconduct previously described:

c. by failing to implement adequate security systems, protocols and practices sufficient to protect Plaintiff's and Class members' PCD both before and after learning of the Data Breach;

d. by failing to comply with industry standard data security standards during the period of the Data Breach; and

e. by failing to timely and accurately disclose that Plaintiff's and Class members' PCD had been improperly acquired or accessed.

95. Through TFCU's and/or UMPP's acts and omissions described in this Petition, including their failure to provide adequate security and its failure to protect Customer Data of Plaintiffs and Class members from being foreseeably captured, accessed, disseminated, stolen and misused, Defendants unlawfully breached their respective duties to use reasonable care to

adequately protect and secure the PCD of Plaintiff and Class members during the time it was within Defendants' possession or control.

96. The law further imposes an affirmative duty on TFCU and/or UMPP to timely disclose the unauthorized access and theft of the PCD to Plaintiff and the Class so that they can take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuse of their PCD, including PII.

97. Defendants each breached their duty to notify Plaintiff and Class Members of the unauthorized access by waiting to notify Plaintiff and Class members and then by failing to provide Plaintiff and Class members sufficient information regarding the breach, including the identity of UMPP; TFCU has not provided sufficient information to Plaintiff and Class members regarding the extent of the unauthorized access and continues to breach its disclosure obligations to Plaintiff and the Class.

98. Defendants' conduct was grossly negligent and departed from all reasonable standards of care, including, but not limited to: failing to adequately protect the Customer Data; failing to conduct regular security audits; failing to provide adequate and appropriate supervision of persons having access to PCD of Plaintiff and Class members.

99. Neither Plaintiff nor the other Class members contributed to the Data Breach and subsequent misuse of their PCD as described in this Petition.

100. The conduct of Defendants TFCU and UMPP complained of herein is the direct and proximate cause of injury and damages incurred by the Plaintiff and the members of the proposed Class, including but not limited to: damages arising from the unauthorized charges on their debit or credit cards or on cards that were fraudulently obtained through the use of the PCD of Plaintiffs and Class members; damages arising from Plaintiff's inability to use their debit or

credit cards because those cards were cancelled, suspended, or otherwise rendered unusable as a result of the Data Breach and/or false or fraudulent charges stemming from the Data Breach, including but not limited to late fees charged and foregone cash back rewards; loss of benefits for PTO; damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives including, *inter alia*, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions. closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, filing police reports and damages from identity theft, which may take months if not years to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy.

101. The nature of other forms of economic damage and injury may take years to detect, and the potential scope can only be assessed after a thorough investigation of the facts and events surrounding the theft mentioned above.

COUNT II
Negligence Per Se
(On Behalf of Plaintiff and the Class)

102. Plaintiff and members of the Class incorporate the above allegations as if fully set forth herein.

103. Pursuant to the FTC Act, 15 U.S.C. § 45, Defendants had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff and members of the Class's PCD.

104. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendants, of failing to use reasonable measures to protect customers' PCD. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of

Defendants' duty to protect Plaintiff and the members of the Class's sensitive PCD.

105. Defendants violated their duty under Section 5 of the FTC Act by failing to use reasonable measures to protect their customers' PCD and not complying with applicable industry standards as described in detail herein. Defendants' conduct was particularly unreasonable given the nature and amount of PCD Defendants had collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to its customers in the event of a breach, which ultimately came to pass.

106. The harm that has occurred is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and members of the Class.

107. Defendants had a duty to Plaintiff and the members of the Class to implement and maintain reasonable security procedures and practices to safeguard Plaintiff's and the Class's PCD.

108. Defendants breached their duties to Plaintiff and members of the Class under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and members of the Class's PCD.

109. Further, Defendants violated the Safeguards Rule of the Gramm-Leach-Bliley Act by failing to use reasonable measures to protect PCD and not complying with industry standards, as described herein.

110. Defendants' violations of Section 5 of the FTC Act and the Safeguards Rule, and its failure to comply with applicable laws and regulations constitute negligence per se.

111. But for Defendants' wrongful and negligent breach of its duties owed to Plaintiff and members of the Class, Plaintiff and members of the Class would not have been injured.

112. The injury and harm suffered by Plaintiff and members of the Class were the reasonably foreseeable result of Defendants' breach of their duties. Defendants knew or should have known that Defendants were failing to meet their duties and that their failure would cause Plaintiff and members of the Class to suffer the foreseeable harms associated with the exposure of their PCD.

113. Had Plaintiff and members of the Class known that Defendants did not adequately protect their PCD, Plaintiff and members of the Class would not have done business with Defendants in the first place.

114. As a direct and proximate result of Defendants' negligence *per se*, Plaintiff and members of the Class have suffered harm, including loss of time, PTO and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; lost control over PCD; unreimbursed losses relating to fraudulent charges; losses relating to exceeding credit and debit card limits and balances; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen PCD, entitling them to damages in an amount to be proven at trial.

COUNT III
Breach of an Implied Contract
(On Behalf of Plaintiff and the Class)

115. Plaintiff and members of the Class incorporate the above allegations as if fully set forth herein.

116. Defendant TFCU offered the Plaintiff and members of the Class banking services in exchange for their entrustment of money to it. Defendant UMPP offered to facilitate transactions between Plaintiff and the Class and various providers of goods and services.

117. In turn, and through internal policies, Defendant TFCU agreed it would not disclose

sensitive banking information to unauthorized persons. Defendant UMPP also promised to safeguard the PCD that it collected and maintained.

118. Plaintiff and the members of the Class accepted Defendants' offers by banking with TFCU and doing business with UMPP.

119. Implicit in the parties' agreements was that Defendants would adequately safeguard the PCD entrusted to them and would provide Plaintiff and members of the Class with prompt and adequate notice of all unauthorized access and/or theft of their PCD.

120. Plaintiff and the members of the Class would not have done business with Defendants in the absence of such agreements with them.

121. Defendants materially breached the contract(s) they had entered with Plaintiff and members of the Class by failing to safeguard such information and failing to adequately notify them of the intrusion into its computer systems that compromised such information. Defendants further breached the implied contracts with Plaintiff and members of the Class by:

a. Failing to properly safeguard and protect Plaintiff and members of the Class's PCD;

b. Failing to comply with industry standards as well as legal obligations that are necessarily incorporated into the parties' agreement; and

c. Failing to ensure the confidentiality and integrity of PCD that Defendants created, received, maintained, and transmitted.

122. The damages sustained by Plaintiff and members of the Class as described above were the direct and proximate result of Defendants' material breaches of its agreement(s).

123. Plaintiff and members of the Class have performed as required under the relevant agreements, or such performance was waived by the conduct of Defendants.

124. The covenant of good faith and fair dealing is an element of every contract. All

such contracts impose upon each party a duty of good faith and fair dealing. The parties must act with honesty in fact in the conduct or transactions concerned. 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.

125. Subterfuge and evasion violate the obligation of good faith in performance even when an actor believes their conduct to be justified. Bad faith may be overt or may consist of inaction, and fair dealing may require more than honesty.

126. Defendants failed to advise Plaintiff and members of the Class of the Data Breach promptly and sufficiently.

127. In these and other ways, Defendants violated its duty of good faith and fair dealing.

128. Plaintiff and members of the Class have sustained damages because of Defendants' breaches of their agreements, including breaches thereof through violations of the covenant of good faith and fair dealing.

COUNT IV
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

129. Plaintiff and members of the Class incorporate the above allegations as if fully set forth herein.

130. This claim is pleaded in the alternative to the breach of implied contractual duty claim.

131. Plaintiff and members of the Class conferred a benefit upon Defendants by banking and/or doing business with them.

132. Defendants appreciated or had knowledge of the benefits conferred upon themselves by Plaintiff and members of the Class. Defendant UMPP also benefited from the receipt of Plaintiff and members of the Class's PCD, as this was used to facilitate transactions with various merchants.

133. Under principals of equity and good conscience, Defendants should not be permitted to retain the full value of the monetary benefit they attained at Plaintiff's and the Class's expense because Defendants failed to adequately protect their PCD. Plaintiff and the proposed Class would not have banked with/done business with Defendants had they known Defendants would not adequately protect their PCD.

134. Defendants should be compelled to disgorge into a common fund for the benefit of Plaintiff and members of the Class all unlawful or inequitable proceeds received by it because of its misconduct and the resulting Data Breach.

COUNT V
Declaratory/Injunctive Relief
(On Behalf of Plaintiff and the Class)

135. Plaintiff and members of the Class incorporate the above allegations as if fully set forth herein.

136. As previously alleged, Plaintiff and Class members entered into an implied contract that required them to provide adequate security for PCD it collected from their payment card transactions. As previously alleged, Defendants owe duties of care to Plaintiff and Class members that require them to adequately secure PCD.

137. Defendants still possess PCD pertaining to Plaintiff and Class members.

138. Defendants have made no announcement or notification that they have remedied the vulnerabilities in their computer data systems.

139. Accordingly, Defendants have not satisfied their contractual obligations and legal duties to Plaintiff and Class members. In fact, now that Defendants' lax approach towards data security is public knowledge, the PCD in their possession is more vulnerable now than ever before.

140. Actual harm has arisen in the wake of the Data Breach regarding Defendants' contractual obligations and duties of care to provide data security measures to Plaintiff and Class members.

141. Plaintiff therefore seeks a declaration that: (a) Defendants' existing data security measures do not comply with their contractual obligations and duties of care, and (b) in order to comply with their contractual obligations and duties of care, Defendants must implement and maintain reasonable security measures, including, but not limited to:

a. engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;

b. engaging third-party security auditors and internal personnel to run automated security monitoring;

c. auditing, testing, and training its security personnel regarding any new or modified procedures;

d. segmenting customer data by, among other things, creating firewalls and access controls so that if one area of Defendants' systems is compromised, hackers cannot gain access to other po1tions of Defendants' systems;

e. purging, deleting, and destroying in a reasonable secure manner PCD not necessary for its provisions of services;

f. conducting regular database scanning and securing checks;

g. routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

h. educating its customers about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps Defendants' customers must take to protect themselves.

COUNT VI
Violation of the Oklahoma Consumer Protection Act (15 O.S. § 751 *et seq.*)
(On Behalf of Plaintiff and the Class)

142. Plaintiff and members of the Class incorporate the above allegations as if fully set forth herein.

143. In failing to promptly, fully and adequately disclose details surrounding the Data Breach, including the identity of UMPP to its customers, Defendant TFCU has violated the Oklahoma Consumer Protection Act ("OCPA").

144. Further, in its characterizations of the Data Breach, Defendant TFCU utilized deceptive practices by – and through – its Breach Notice to Plaintiff and members of the Class.

145. Defendant TFCU utilized unfair trade practices in representing the nature of the Data Breach as well as its purported efforts to rectify the Data Breach.

146. As detailed herein, Defendant TFCU made false or misleading representations to Plaintiff and members of the Class as to the nature, characteristics, uses, and benefits of Defendant's purported efforts to rectify the Data Breach.

147. Since the OCPA parallels the FTC Act, Defendants' violations of the FTC Act explained, *supra*, constitute a violation of the OCPA too; especially those violations of the FTC

Act concerning data security.

148. Defendants utilized these and other deceptive and unfair practices to work an unfair advantage over Plaintiff and members of the Class.

149. Plaintiff and member of the Class have incurred damages as a result of Defendant's violations of the OCPA.

COUNT VII
Invasion of Privacy
(On Behalf of Plaintiff and the Class)

150. Plaintiff and members of the Class incorporate the above allegations as if fully set forth herein.

151. Defendants published Plaintiff's and Class members' PCD, which constitutes private details and facts not generally known to the public, not publicly available, and not of legitimate public concern about Plaintiff and Class members by disclosing and exposing Plaintiff's and Class members' private and sensitive PCD to enough people that it is reasonably likely those facts will become known to the public at large, including without limitation on the dark web and elsewhere.

152. Plaintiff's and Class members' PCD, which included credit and debit card numbers as well as cardholder names, account numbers, expiration dates, card verification values, and PIN data for debit cards, was private and intimate.

153. Defendants' disclosure of the PCD unreasonably, substantially and seriously interfered with Plaintiff's and Class members' privacy and ordinary sensibilities. Defendant should appreciate that the cyber-criminals who stole the PCD would further sell and disclose the PCD as they are doing and as they did. That the original disclosure is devastating to Plaintiff and Class members even though it may have originally only been made to one person or a limited number of

cyber-criminals (although Defendant TFCU failed to disclose who stole the PCD) does not render it any less a disclosure to the public-at-large.

154. The tort of public disclosure of private facts is recognized in Oklahoma. Plaintiff's and Class members' private and sensitive PCD was publicly disclosed by Defendants in the Data Breach with reckless disregard for the offensiveness of the disclosure. Such disclosure is highly offensive and would be to any person of ordinary sensibilities. Defendants knew and know that Plaintiff's and Class members' PCD is not a matter of legitimate public concern. As a direct and proximate result of Defendants' conduct, Plaintiff and Class members have been injured and are entitled to damages.

PRAYER FOR RELIEF

Plaintiff and members of the Class demand a jury trial on all claims so triable and request that the Court enter an order:

A. Certifying this case as a class action on behalf of Plaintiff and the proposed Class, appointing Plaintiff as class representative, and appointing her counsel to represent the Class;

B. Awarding declaratory and other equitable relief as is necessary to protect the interests of Plaintiff and the Class;

C. Awarding injunctive relief as is necessary to protect the interests of Plaintiff and the Class;

D. Enjoining Defendants from further deceptive practices and making untrue statements about the Data Breach and the stolen PHI and PII;

E. Awarding Plaintiff and the Class damages that include applicable compensatory, exemplary, punitive damages, as allowed by law;

F. Awarding restitution and damages to Plaintiff and the Class in an amount to be determined at trial;

G. Awarding attorneys' fees and costs, as allowed by law;

H. Awarding prejudgment and post-judgment interest, as provided by law;

I. Granting Plaintiff and the Class leave to amend this Petition to conform to the evidence produced at trial; and

J. Granting such other or further relief as may be appropriate under the circumstances.

JURY DEMAND

Plaintiff demands a trial by jury on all issues so triable.

RESPECTFULLY SUBMITTED AND DATED this 12th day of October, 2022.

Jason B. Aamodt, OBA No. 16974
Matthew D. Alison, OBA No. 32723
INDIAN & ENVIRONMENTAL LAW GROUP, PLLC
406 South Boulder Ave., Suite 830
Tulsa, OK 74103
Telephone: (918) 347-6169
Facsimile: (918) 948-6190

Lynn A. Toops, (pro hac vice forthcoming)
Amina A. Thomas, (pro hac vice forthcoming)
COHEN & MALAD, LLP
One Indiana Square, Suite 1400
Indianapolis, IN 46204
ltoops@cohenmalad.com
athomas@cohenmalad.com

J. Gerard Stranch, IV, (pro hac vice forthcoming)
Peter J. Jannace, (pro hac vice forthcoming)
BRANSTETTER, STRANCH & JENNINGS, PLLC
223 Rosa L. Parks Ave. Suite 200

Nashville, TN 37203
gerards@bsjfirm.com
peterj@bsjfirm.com

Attorneys for Plaintiff

ClassAction.org
