EFILED 02/08/23 06:33 AM CASE NO. 23C303 Joseph P. Day, Clerk

IN THE CIRCUIT COURT OF DAVIDSON COUNTY, TENNESSEE FOR THE TWENTIETH JUDICIAL DISTRICT AT NASHVILLE

JOSIAH AREND, and BREANNA AREND, individually, and on behalf of all others similarly situated, *Plaintiffs*, v. NEWCOURSE COMMUNICATIONS, INC. -and- FIRST UNITED BANK AND TRUST CO. *Defendants*.	)	Case No.

CLASS ACTION COMPLAINT

Plaintiffs, JOSIAH AREND, and BREANNA AREND (collectively, "Plaintiffs"), individually, and on behalf of all others similarly situated, bring this class action against Defendants, NEWCOURSE COMMUNICATIONS, INC. ("Newcourse"), and FIRST UNITED BANK & TRUST CO. ("FUB") (collectively, "Defendants") alleging as follows:

INTRODUCTION

1. This is a civil action seeking monetary damages, and injunctive and declaratory relief, from the Defendant(s), Newcourse Communications, Inc., a Nashville printing company providing services to financial and other institutions across the United States, and First United Bank and Trust Co., an Oklahoma domestic bank, arising from their collective failure to safeguard the highly-sensitive personal information, Personally Identifiable Information ("PII")[1], of

[1] 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,

thousands of persons, including Plaintiffs and the proposed Class Members, resulting in a data breach to Newcourse's systems from April 27, 2022 to May 3, 2022 in which that PII was unauthorizedly disclosed to cybercriminals, causing widespread injury and monetary damages.

2. As follows hereinafter, Newcourse provides printing services to companies and financial institutions, including FUB, as well as Old National Bank, Tennessee Housing Development Agency d/b/a Volunteer Mortgage Loan Servicing, OwnersChoice Funding, Inc., and others.

3. On information and belief, from April 27, 2022 to May 3, 2022 cybercriminals were able to unauthorizedly access Newcourse's computer networks in an external system breach hacking attack, and remove the PII of thousands of persons, including Plaintiffs and the proposed Class Members, including their full names, addresses, loan account number, and the last four digits of their Social Security Numbers and/or myriad other personal and financial information (the "Data Breach").[2]

4. The Data Breach was caused by Defendants' acts and omissions in failing to adequately protect Plaintiffs' and the proposed Class Members' PII.

5. As a result of the Data Breach, Plaintiffs and the Class Members have been caused serious harm including fraudulent activity and identity theft, and suffered widespread damages.

6. Plaintiffs are each FUB customers whose PII was in the custody of Newcourse and

---

government passport number, employer or taxpayer identification number." 17 C.F.R. § 248.201(b)(8). To be clear, according to Defendants, not every type of information included in that definition was compromised in the Data Breach.

[2] *See*: Newcourse Communications, Inc., "Newcourse Data Breach Notice to Josiah Arend" dated October 31, 2022, **attached as Exhibit A**; "Newcourse Data Breach Notice to Breanna Arend," Oc. 31, 2022, **Exhibit B**; and, sample Newcourse Communications, Inc., Notice to California Attorney General, available at https://oag.ca.gov/ecrime/databreach/reports/sb24-558699 (last accessed Feb. 4, 2023), **Exhibit C.**

are both Data Breach victims, and bring this class action on behalf of themselves, and all victims of Defendants' tortious misconduct and breach of contractual obligations whose PII was unauthorizedly disclosed in Newcourse's Data Breach.

PARTIES

7. Plaintiff, Josiah Arend, is an Oklahoma citizen residing in Owasso, Oklahoma, in Tulsa County, where he intends to remain. He is a Data Breach victim, as evident from the facts, as follow below.

8. Plaintiff, Breanna Arend, is an Oklahoma citizen residing in Owasso, Oklahoma, in Tulsa County, where she intends to remain. She is a Data Breach victim, as evident from the facts, as follow below, and Josiah Arend's spouse.

9. Defendant Newcourse is a corporation organized and existing under the laws of the State of Tennessee, with a principal place of business located at 5010 Linbar Drive, Suite 100, Nashville, Tennessee 37211 in Davidson County. Newcourse's Registered Agent for Service of Process is James Conde, 5010 Linbar Drive, Ste. 100, Nashville, TN 37211.

10. Defendant FUB is a bank and trust company organized and existing under the laws of the State of Oklahoma, with a principal place of business located at 1400 West Main Street, Durant, Oklahoma 74701 in Bryan County. FUB's Registered Agent for Service of Process is Spend Life Wisely Company, Inc., 1400 West Main Street, Durant Oklahoma 74701

JURISDICTION & VENUE

11. This Court has personal jurisdiction over Newcourse pursuant to Tenn. Code § 20-2-222 as said Defendant is domiciled in, organized under the laws of, and maintains a principal place of business in Tennessee.

12. The Court has personal jurisdiction over FUB pursuant to Tenn. Code § 20-2-223

as FUB contracted with Newcourse in Tennessee to supply mailing services for FUB.

13. The Court has subject matter jurisdiction pursuant to Tenn. Code § 16-10-101.

14. Venue is proper in Davidson County pursuant to Tenn. Code § 20-4-104 as the county where Newcourse maintains its principal place of business.

BACKGROUND FACTS

A. Defendant Newcourse

15. Newcourse is a commercial printing company located in Nashville, Tennessee, established in 2005, which provides "full-service data-processing, print-&-mail" services to companies, primarily financial institutions. Newcourse:

> …specializes in custom jobs for the mortgage, automobile, credit union and banking industries by delivering custom programming, creative services and production solutions for clients who are on various servicing software systems including BKFS, FICS, Megasys, and in-house platforms.[3]

16. Newcourse's services include: 1st mortgage monthly billing periodic statements; initial analysis statements, annual 1098 year-end statements, check books, annual FHA prepayment notifications, transfer of servicing letters, hazard insurance reminders and renewals, prime commercial billing statements, HELOC convenience check books, payment books, delinquent statements, 2nd mortgage HELOC and LOC billing statements, adjustable rate mortgage (arm) letters, draft forms, mortgagee clause change requests, late charge billings, IRS 1099a, 1099c, 1099int & 1099misc forms, bulk and individual images for long term archival in PDF or TIF formats, electronic bill presentment & payment (EBPP), **annual privacy policy notification,** transmissions for activity updates, 10-day, 15-day, 30-day, 45-day and 60-day delinquency notices, audit confirmations, default and loss mitigation letters, paid-in-full and

[3] Newcourse Communications, Inc., Website, https://www.newcoursecc.com/page/about (last accessed Feb. 4, 2023).

interest-on-escrow checks, annual or short year escrow analysis statement with surplus checks, and W9 verification of Social Security Numbers and Tax Identification Numbers.[4]

17. Newcourse provides printing services to financial institutions and other companies, including FUB[5] in Oklahoma and Texas, as well as to Old National Bank[6], Tennessee Housing Development Agency d/b/a Volunteer Mortgage Loan Servicing[7], OwnersChoice Funding, Inc.[8], and HomeStreet Bank[9] and others.

18. Newcourse collects personal information, PII, of these institutions' customers, Plaintiffs and the proposed Class Members, including their names, addresses, loan account numbers, Social Security Numbers, and other information, all of which it stores on its computer systems.

19. As follows hereinafter, upon information and belief, as early as August 5, 2022 Newcourse discovered that from April 27, 2022 to May 3, 2022, approximately, its computer networks had been unauthorizedly accessed in an external system breach hacking attack, resulting in the removal of PII stored on those systems of Plaintiffs and the proposed Class Members by

---

[4] *Id*.
[5] *See* Newcourse Communications, Inc., "Newcourse Data Breach Notice to Josiah Arend" October 31, 2022, Ex. A; "Newcourse Data Breach Notice to Breanna Arend," Ex. B.
[6] *See*: Newcourse Communications, Inc., sample Notice of Data Breach, August 18, 2022, New Hampshire Attorney General, available at https://www.doj.nh.gov/consumer/security-breaches/documents/newcourse-communications-20220825.pdf (last accessed Feb. 4, 2023).
[7] *See*: Newcourse Communications, Inc., sample Notice of Data Breach, October 19, 2022, New Hampshire Attorney General, available at https://www.doj.nh.gov/consumer/security-breaches/documents/newcourse-communications-20221024.pdf (last accessed Feb. 4, 2023).
[8] *See*: Newcourse Communications, Inc., sample Notice of Data Breach, November 4, 2022, New Hampshire Attorney General, available at https://www.doj.nh.gov/consumer/security-breaches/documents/newcourse-communications-20221107.pdf (last accessed Feb. 4, 2023).
[9] *See Newcourse Communications, Inc*., sample Notice of Data Breach, California Attorney General, available at https://oag.ca.gov/system/files/Newcourse%20Communications%20-%20Homestreet%20Bank%20-%20Final%20Notice%20Letter%20Version%20%5Bredacted%5D%20%2810635980x7AB84%29.pdf (last accessed Feb. 4, 2023).

cybercriminals, the Data Breach.[10]

20. The Data Breach resulted in the unauthorized disclosure of the PII of Plaintiff and the proposed Class Members, causing legally cognizable injury and damages as set forth herein.

21. Despite recognizing the risk of identity theft due to stolen PII and other personal information, and despite its duties to protect that information, Newcourse 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 FUB

22. FUB is an Oklahoma banking and trust company headquartered in Durant, Oklahoma which provides services to over 300,000 customers across Oklahoma and Texas[11] and with $14.5 billion in assets.[12]

23. FUB holds itself out as "…not your typical bank. [It is] driven by a higher purpose and guided by a core set of values that inspire us to serve all of our stakeholders."[13] FUB states that its purpose is "[t]o inspire and empower others to *Spend Life Wisely,"* and espouses values of faith, family, and integrity.[14]

24. Upon information and belief, FUB operates eighty (80) locations across Oklahoma

---

[10] See: Newcourse Communications, Inc., sample Notice of Data Breach, August 18, 2022, to the New Hampshire Attorney General, available at https://www.doj.nh.gov/consumer/security-breaches/documents/newcourse-communications-20220825.pdf (last accessed Feb. 2, 2023);
[11] First United Bank Website, available at https://www.firstunitedbank.com/ (last accessed February 2, 2023), *see* Annual Report, pg. 8, https://trabian-canvas-prd-files.s3.amazonaws.com/firstunitedbank-com/files/document/first-united-annual-report-2022-single.pdf, https://www.firstunitedbank.com/locations.
[12] *See* Annual Report, pg. 8, https://trabian-canvas-prd-files.s3.amazonaws.com/firstunitedbank-com/files/document/first-united-annual-report-2022-single.pdf, pg. 9.
[13] First United Bank Website https://www.firstunitedbank.com/about-us.
[14] First United Bank Website https://www.firstunitedbank.com/about-us.

and Texas in sixty (60) communities, in Oklahoma in Durant, Calera, Colbert, Bokchito, Kingston, Tishomingo, Madill, Hugo, Ada, Pauls Valley, Holdenville, Wewoka, Maysville, Seminole, Purcell, Tecumseh, Shawnee, Norman, Moore, Oklahoma City, Edmond, and Sapulpa, Oklahoma; and in Texas in Denison, Pottsboro, Sherman, Sherman, Bonham, Whitesboro, Leonard, Gainesville, McKinney, Prosper, McKinney, Sanger, Frisco, Denton, Plano, Krum, and in Dallas, Texas.[15]

25. FUB provides customers with services including depository bank, checking, and savings accounts, certificates of deposit, secure checking services, debit card services, ATMs, lending services including consumer and personal loans, mortgages, lines of credit, as well as insurance products, estate planning, investment management, retirement planning and trust services.[16]

26. As a material condition of providing customers with financial services, FUB collects personal information, PII, of customers including their names, addresses, loan account number, Social Security Numbers, as well as other information including credit history, account balances, payment history, transaction history, and account transactions[17], all of which it stores on its computer systems.

27. FUB maintains a Consumer Privacy Policy, providing how Defendant collects, shares, and protects PII, including "to share customers' personal information to run their everyday business," "such as to process [] transactions, maintain [] account(s), respond to court orders and

[15] First United Bank Website, "Locations," available at https://www.firstunitedbank.com/locations.
[16] *See id.*
[17] First United Bank, Consumer Privacy Policy, available at https://www.firstunitedbank.com/privacy-policy.

legal investigations, or report to credit bureaus."[18]

28. FUB's Consumer Privacy further provides it may disclose PII for its "affiliates' everyday business purposes." "Affiliate" is defined as "Companies related by common ownership or control. They can be financial and non-financial companies. [FUB's] affiliates include: Financial companies such as: Finotta, Exencial Wealth Management, and First United Bank Insurance Solutions, Inc." Accordingly, Newcourse is not FUB's Affiliate.

29. The Data Breach is not included in the authorized purposes for FUB disclosing its customers' PII pursuant to its Consumer Privacy Policy.

30. In offering financial services to customers, FUB acknowledges the risks posed by identity theft of PII, representing and warranting to consumers in its Consumer Privacy Policy that:

> To protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer safeguards and secured files and buildings. We also maintain other physical, electronic and procedural safeguards to protect this information and we limit access to information to those employees for whom access is appropriate.[19]

31. Despite recognizing the risk of identity theft that can result from stolen PII, and despite its duties to protect that information, FUB does not follow industry standard practices in ensuring that its vendors take adequate measures to secure that PII.

32. FUB utilizes Newcourse to perform printing services in connection with its financial services to consumers.

33. On information and belief, FUB knew of Newcourse's deficient security practices, and nevertheless, by acts of commission or omission, permitted Newcourse to receive the PII of its customers, including Plaintiffs and the proposed Class members, to perform mailing services,

---

[18] *See* First United Bank, Consumer Privacy Policy, available at https://www.firstunitedbank.com/privacy-policy (last accessed Feb. 4, 2023).
[19] *See id.*

despite purported privacy policies which would not appear to allow any such disclosure.

C. Newcourse and FUB Failed to Safeguard Plaintiffs' and Class Members' PII

34. Plaintiffs and Class Members are victims whose was PII was entrusted to Newcourse by their financial and other institutions, including but not limited to FUB, and unauthorizedly disclosed in the Data Breach to Newcourse, resulting in widespread injury and damages.

35. As described herein, Newcourse's data security safeguards are inadequate to protect the vast amounts of PII received from these financial and other institutions including FUB, collected, stored, and utilized; and, FUB's data security safeguards relating to its vendors, Newcourse, are inadequate to protect its customer's PII.

36. Upon information and belief, from April 27, 2022 to May 3, 2022 the PII of Plaintiffs and the members of the proposed Class stored Newcourse's computer systems was unauthorizedly accessed, removed by, and disclosed to third party cybercriminals whose sole purpose was the imminent fraudulent and criminal misuse of that PII ("the Data Breach").[20]

37. Subsequent to the foregoing, according to Newcourse, it "immediately launched an investigation in consultation with outside cybersecurity professionals who regularly investigate and analyze these types of situations to analyze the extent of any compromise of the information on our network."[21]

38. It is unknown what, if any, measures Newcourse undertook to secure its systems following the Data Breach.

[20] *See* Newcourse's Notices to Plaintiffs, Ex. A, B; as well as the same or similar sample data breach notices, e.g., California Attorney General, Ex. C.
[21] *See Id.*

39. On information and belief, on or about August 18, 2022, Newcourse began notifying affected customers that Newcourse had discovered that the customer's PII, including names and Social Security Numbers, had been compromised and unauthorizedly disclosed in the Data Breach.[22]

40. By letter dated August 17, 2022, Newcourse notified the New Hampshire Attorney General of the Data Breach as to the unauthorized disclosure of PII of impacted customers.[23] In Newcourse's August 19, 2022 report to the Maine Attorney General, it reported the breach as involving 47,970 persons, and stated that consumers were being notified of the Data Breach in writing as of August 18, 2022.[24]

41. On information and belief, on or about October 20, 2022, Newcourse began notifying other or additional affected customers, advising that on September 20, 2022 Newcourse had discovered that their PII had been compromised and unauthorizedly disclosed in the Data Breach. [25]

42. On October 19, 2022, Newcourse notified the New Hampshire Attorney General of

---

[22] *See*: Maine Attorney General, Data Breach Notifications, August 16, 2022, and Newcourse's Sample Notice of Data Breach, Maine Attorney General, August 18, 2022, available at https://apps.web.maine.gov/online/aeviewer/ME/40/723f7327-59b4-49d1-b655-af2f6de4e261.shtml.

[23] *See*, McDonald Hopkins LLC, Letter to New Hampshire Attorney General, August 17, 2022, attached as **Exhibit D.**

[24] *See*: Maine Attorney General, Data Breach Notifications, August 16, 2022; and Newcourse sample Notice of Data Breach, August 18, 2022, available at https://apps.web.maine.gov/online/aeviewer/ME/40/723f7327-59b4-49d1-b655-af2f6de4e261.shtml (last accessed on Feb. 4, 2022).

[25] *See*: Maine Attorney General, Data Breach Notifications, and Newcourse sample Notice of Data Breach, available at https://apps.web.maine.gov/online/aeviewer/ME/40/795fa028-72c4-4c69-acaa-e7dc5d203d4e.shtml (last accessed on Feb. 4, 2022); McDonald Hopkins LLC, Letter to New Hampshire Attorney General, October 19, 2022, and sample Notice of Data Breach, attached as **Exhibit E.**

the Data Breach[26]; and reported to the same to the Maine Attorney General on or about October 23, 2022, as discovered on September 20, 2022, involving 35,266 persons whose names and Social Security Numbers were compromised, and stating that affected consumers were being notified as of October 20, 2022.[27]

43. On information and belief, on or about November 4, 2022, Newcourse began notifying other or additional affected customers, advising that on October 5, 2022 Newcourse had discovered that their PII had been compromised and unauthorizedly disclosed in the Data Breach.[28]

44. On or about October 29, 2022, Newcourse notified the Maine Attorney General of the Data Breach involving 13,897 affected customers whose names and Social Security Numbers were compromised, advising that the Data Breach was discovered on October 5, 2022, and that affected consumers were being notified on November 4, 2022. [29]

45. On or about October 31, 2022, Newcourse notified the New Hampshire Attorney General of the Data Breach, as well.[30]

46. On or about November 19, 2022, Newcourse notified the Maine Attorney General of a total of 77,304 persons impacted in the Data Breach, "which includes previously reported

---

[26] *See*: McDonald Hopkins LLC, Letter to New Hampshire Attorney General, October 19, 2022, and sample Notice of Data Breach, Ex. E.
[27] *See* Maine Attorney General, Data Breach Notifications, and sample Notice of Data Breach, available at https://apps.web.maine.gov/online/aeviewer/ME/40/795fa028-72c4-4c69-acaa-e7dc5d203d4e.shtml (last accessed on Feb. 4, 2022).
[28] *See*: McDonald Hopkins LLC, Letter to New Hampshire Attorney General, October 31, 2022, and sample Notice of Data Breach, attached as **Exhibit F**; Maine Attorney General, Data Breach Notifications, October 29, 2022, sample Notice of Data Breach, November 4, 2022, available at https://apps.web.maine.gov/online/aeviewer/ME/40/5a7971f2-4c3d-4a6c-9d32-de583922d13f.shtml (last accessed on Feb. 4, 2022).
[29] *See*: Maine Attorney General, Data Breach Notifications, October 29, 2022, available at https://apps.web.maine.gov/online/aeviewer/ME/40/5a7971f2-4c3d-4a6c-9d32-de583922d13f.shtml (last accessed on Feb. 4, 2022).
[30] *See*: McDonald Hopkins LLC, Letter to New Hampshire Attorney General, October 31, 2022, and sample Notice of Data Breach, Ex. F.

47,970 affected individuals reported to the AG on August 19, 2022."[31]

47. On information and belief, on or about September 10, 2022 Newcourse began notifying other or additional affected customers, advising that on August 21, 2022 Newcourse discovered that their PII had been compromised and unauthorizedly disclosed in the Data Breach, including full names, loan account number, details included on a 1098 mortgage statement, address, loan balance, loan interest paid, and the last four digits of Social Security numbers.[32]

48. Beginning on or about October 31, 2022, Newcourse began notifying affected customers of it and FUB, including Plaintiffs, that on October 18, 2022 Newcourse had discovered that their PII had been compromised and unauthorizedly disclosed in the Data Breach, including their full names, as well as their addresses, loan numbers, and last four digits of Social Security Numbers.[33]

49. On or about October 28, 2022, Newcourse reported the Data Breach to the California Attorney General as to FUB customers.[34]

---

[31] Maine Attorney General, Data Breach Notifications, available at https://apps.web.maine.gov/online/aeviewer/ME/40/3ddc88fd-b892-4272-babb-fceab5be1ba5.shtml (last accessed on Feb. 4, 2022).

[32] *See Newcourse Communications, Inc*., sample Notice of Data Breach, California Attorney General, available at https://oag.ca.gov/system/files/Newcourse%20Communications%20-%20Homestreet%20Bank%20-%20Final%20Notice%20Letter%20Version%20%5Bredacted%5D%20%2810635980x7AB84%29.pdf.

[33] *See* Newcourse Communications, Inc., Newcourse Data Breach Notice to Josiah Arend, October 31, 2022, attached as Ex. A; "Newcourse Data Breach Notice to Breanna," Ex. B; sample Notice to California Attorney General, available at https://oag.ca.gov/ecrime/databreach/reports/sb24-558699 (Ex. C) (last accessed on Feb. 4, 2022).

[34] *See* Data Security Breaches, "Newcourse Communications," California Attorney General website, available at https://oag.ca.gov/privacy/databreach/list?field_sb24_org_name_value=newcourse&field_sb24_breach_date_value%5Bmin%5D%5Bdate%5D=&field_sb24_breach_date_value%5Bmax%5D%5Bdate%5D= (last accessed on Feb. 4, 2022).

50. Newcourse's October 31, 2022 Notice of the Data Breach to Plaintiffs informed them that "recently" Newcourse had discovered the Data Breach from April 27, 2022 and May 3, 2022, which on October 18, 2022 was found to have resulted in removal of Plaintiffs' PII.[35]

51. Newcourse's foregoing notices, which are substantially identical aside from the dates the Data Breach was discovered (collectively, "Data Breach Notices"), failed to apprise Plaintiffs and the Class as to details as to how the Data Breach occurred—via an external system breach hacking attack—obfuscating the nature and severity of the breach.

52. As acknowledged by Newcourse throughout its Data Breach Notices, the Data Breach resulted in the PII of Plaintiffs and the proposed Class Members being removed from Newcourse's networks by cybercriminals, including their names, addresses loan account numbers, and the last four digits of his Social Security Number.

53. Despite this, Newcourse' Data Breach Notices represented to Plaintiffs and the Class Members that said Defendant was "… not aware of any reports of identity fraud or improper use of your information as a direct result of this incident."[36]

54. In its Data Breach Notice(s), Newcourse encouraged Plaintiffs and the Class Members to remain vigilant in reviewing their financial account statements and credit reports for any fraudulent or suspicious activity.[37]

55. Further, Newcourse's Data Breach Notice apprised Plaintiffs and the Class Members of precautionary measures they could take to protect their information, including placing a fraud alert or a security freeze on their credit files.

56. In addition, as communicated in Newcourse's Data Breach Notices, Newcourse

[35] *See Id.*
[36] *See generally* Exhibits A-C.
[37] *Id.*

offered Plaintiffs and the Class Members 24 months of complimentary identity theft protection through IDX, with a deadline to enroll of January 31, 2023.[38]

57. This identify theft protection is not sufficient to compensate Plaintiffs and the Class Members for the harm caused by the Data Breach, as follows.

58. As alleged herein, the Data Breach was the direct and proximate result of the collective failures of Defendants to adequately protect the PII of Plaintiffs and the proposed Class Members which was entrusted to it.

59. Despite the abundance and availability of information regarding cybersecurity best practices, Newcourse failed to adopt and employ adequate data security processes to safeguard Plaintiffs' and the Class Members' PII – and FUB failed to ensure that Newcourse implemented adequate data security processes to protect the PII entrusted to its third-party vendor.

60. Newcourse failed to adequately train its employees on even the most basic of cybersecurity protocols, including:

a. How to detect phishing emails and other scams including providing employees examples of these scams and guidance on how to verify if emails are legitimate;

b. Effective password management and encryption protocols for internal and external emails;

c. Avoidance of responding to emails that are suspicious or from unknown sources;

d. Locking, encrypting and limiting access to computers and files containing sensitive information; and,

e. Implementing guidelines for maintaining and communicating sensitive

[38] *Id.*

data.

61. Newcourse's failures to implement these rudimentary measures made it an easy target for the Data Breach described above.

D. Plaintiffs' Experiences

62. Plaintiffs, Josiah Arend and Breanna Arend, are customers of FUB, as borrowers on a home mortgage loan.

63. As a condition of banking with FUB, Plaintiffs were required to provide and entrust to FUB their personal and highly sensitive PII, with the implicit understanding that this PII would be kept confidential. This understanding was based on all the facts and circumstances attendant to Plaintiffs receiving services, and the express, specific, written and oral representations made by FUB and its agents, including in the Consumer Privacy Policy.

64. Plaintiffs reasonably relied upon FUB's representations to their detriment and would not have provided their sensitive PII to FUB if not for Defendant's explicit and implicit promises to adequately safeguard that information.

65. Unknown to Plaintiffs, FUB provided and entrusted their PII to Newcourse, its third-party vendor, in connection with performing printing services for FUB.

66. Plaintiffs received Newcourse's October 31, 2022 Notice of Data Breach[39], as well as FUB's notice of the Data Breach.[40]

67. As Defendants acknowledged in the Data Breach Notices, Plaintiffs' PII was unauthorizedly disclosed in the Data Breach to Newcourse's computer systems, including their full names, addresses, loan account number, and the last four digits of their Social Security

[39] *See* Ex. A, B.
[40] *See* First United Bank, Letter, undated, attached as **Exhibit G.**

Numbers.[41]

68. As Defendants acknowledged in the Data Breach Notices, the Class Members' PII was unauthorizedly disclosed in the Data Breach to Newcourse's computer systems, including their full names, addresses, loan account number, and the last four digits of their Social Security Numbers, as well as other personal and financial information, as communicated in the Data Breach Notices from August 2022 forward.

69. As a result of the Data Breach permitted to occur by Newcourse, Plaintiffs' and the Class Members' PII was disclosed in the public domain, and is now being utilized by cybercriminals for fraudulent and criminal activity, and identity theft, causing Plaintiffs significant injuries and monetary damages.

70. To their knowledge, Plaintiffs have never been involved in a data breach or experienced unauthorized disclosure of their personal information, PII, prior to Newcourse's Data Breach.

71. Following the Data Breach, Josiah Arend's PII, his Social Security Number, was fraudulently used by cybercriminals to open an account with Chase Bank.

72. Thankfully, Plaintiffs were able to detect the fraudulent account opening and are working with Chase Bank to close the fraudulent account, being forced to expend time and labor to do so.

73. Plaintiffs' detection of the fraudulent activity was made all the more difficult because the cybercriminals utilized Josiah Arend's PII, his email address, to enroll in various online platforms and correspondences and, in doing so, flood Mr. Arend's email inbox with junk messages in an effort to bury the criminal's interactions with financial institutions. Mr. Arend

[41] *See* Ex. A, B; *see also* First United Bank, Letter, undated, attached as **Exhibit G**.

would not have learned of the opening of the Chase account as soon as he did, had he not taken the time to wade through the wave of emails, wherein he saw a message from Chase thanking him for opening his new account.

74. In addition, cybercriminals are fraudulently using Plaintiff Josiah Arend's PII to pose as him and attempt to steal monies, including his wages paid via direct deposit. Following the Data Breach, Josiah's prior employer received an email from an unknown person fraudulently using Plaintiff's identity, who claimed that Josiah's bank information had been changed and the employer needed to direct his paychecks to another account.

75. Thankfully, the employee who received the communication personally knew Plaintiff Josiah Arend and contacted him to verify his identity, thwarting the cybercriminals attempted theft.

76. As a result of the Data Breach, Plaintiffs have been forced to expend, and will continue to expend, additional time for changing emails, changing passwords, calling various institutions, freezing their credit, filing a police report, researching/obtaining identity protection & monitoring services, contacting employers regarding paychecks, updating contact information, and changing card and pin numbers.

77. The fraudulent activity to Plaintiffs as a result of the Data Breach is ongoing, and further fraudulent activity will imminently come to pass due to Defendants' failure to prevent the Data Breach.

78. At all relevant times, Newcourse knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiff and the proposed Class Members entrusted to it by its customers, including FUB, 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 Plaintiffs and the proposed Class, as a result of a breach.

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

80. As a direct and proximate result of the Data Breach permitted to occur by Defendant(s), Newcourse and/or FUB, Plaintiffs have each suffered or will imminently suffer significant harms, including ongoing fraudulent misuse of their PII, fraudulent charges and monetary damages, and considerable time and effort to remedy the effects of the Data Breach and prevent further injury, and to monitor their accounts to protect themselves from further identity theft. Plaintiffs fear for their personal financial security and uncertainty. They are 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. Plaintiffs and the Proposed Class Have Suffered Injury and Damages.

81. As described herein, Plaintiffs and members of the proposed Class have suffered injury from the misuse of their PII that can be directly traced to the Data Breach to Newcourse's systems, occurring because of Defendants' collective acts or omissions in failing to secure the PII.

82. The ramifications of Defendant(s)' collective failure to keep Plaintiffs' and the Class's PII 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.

83. As a result of Newcourse failing to prevent the Data Breach, and FUB failing to

ensure that its vendor maintained adequate security systems, Plaintiffs 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. Fraudulent misuse of Plaintiffs' PII to open bank accounts, and attempted theft of monies as described above;

b. Ongoing identity theft;

c. The loss of the opportunity to control how their PII is used;

d. The diminution in value of their PII;

e. The compromise, publication and/or theft of their PII;

f. Out-of-pocket costs associated with the prevention, detection, recovery and remediation from identity theft or fraud, including the purchase of identity theft protection insurance and detection services;

g. Lost opportunity costs and lost wages associated with the time and effort expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from identity theft and fraud;

h. Delay in receipt of tax refund monies;

i. Unauthorized use of stolen PII;

j. The continued risk to their PII, which remains in the possession of Defendants and is subject to further breaches so long as they fail to undertake appropriate measures to protect the PII in their possession; and

k. Current and future costs related to the time, effort, and money that will be expended to prevent, detect, contest, remediate and repair the impact of the Data Breach for the

remainder of the lives of Plaintiffs and Class members.

84. At all relevant times, Defendants were each well-aware, or reasonably should have been aware, that PII 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.

85. It is well known and the subject of many media reports that PII 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 PII of Plaintiffs and the Class Members.

86. PII is a valuable commodity because it contains not only payment card numbers but Personally Identifiable Information ("PII") as well. A "cyber black market" exists in which criminals openly post stolen payment card numbers, social security numbers, and other personal information on multiple underground Internet websites. PII 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.

87. 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.

88. The value of Plaintiffs' and the proposed Class's PII 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.

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

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

91. 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.

92. The development of "Fullz" packages means that stolen PII from the Data Breach can easily be used to link and identify it to Plaintiffs' 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 Plaintiffs and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiffs' and other members of the proposed Class's stolen PII is being misused, and that such misuse is fairly traceable to the Data Breach.

93. 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.[42]

94. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good."

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

95. 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, exactly as occurred with Plaintiffs Josiah and Breanna Arend here.

96. 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, just as occurred with Plaintiffs here.

97. 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, Plaintiffs and the Class will need to remain vigilant against unauthorized data use for years or even decades to come, especially as identity theft attacks are ongoing.

98. 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."[43]

99. The FTC has also issued several guidelines for both businesses and financial

[43]Commissioner Pamela Jones Harbour Remarks Before FTC Exploring Privacy Roundtable Washington, D.C December 7, 2009, available at https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-ftc-exploring-privacy-roundtable/091207privacyroundtable.pdf (Last accessed Feb. 4, 2023).

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.[44]

100. 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.

101. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating 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 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

102. Defendants' collective failures to employ reasonable and appropriate measures to protect against unauthorized access to customers' PII constitutes an unfair act or practice

[44] *See generally Start With Security, A Guide for Business*, FTC, https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

CLASS ACTION ALLEGATIONS

103. Plaintiffs sue on behalf of themselves, and the proposed Class, defined as follows:

> All persons whose PII was disclosed without authorization in the Data Breach experienced by Newcourse from April 27, 2022 to May 3, 2022.

104. The following people are excluded from the Class: (1) any judge or magistrate presiding over this action and members of their families; (2) Defendant, Defendant's subsidiaries, parents, successors, predecessors, affiliated entities, and any entity in which Defendant or its parent has a controlling interest, and their current or former officers and directors; (3) persons who properly execute and file a timely request for exclusion from the Class; (4) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (5) Plaintiffs' counsel and Defendant's counsel; and (6) the legal representatives, successors, and assigns of any such excluded persons.

105. The Class defined above is identifiable through Defendants' business records.

106. Plaintiffs reserve the right to amend the class definition.

107. This action satisfies the numerosity, commonality, typicality, and adequacy requirements under Tenn. R. Civ. P. 23.01.

108. **Numerosity**. Plaintiffs are the representatives of the proposed Class, consisting of thousands of members, far too many to join in a single action;

109. **Typicality**. Plaintiffs' claims are typical of Class member's claims as each arises from the same Data Breach, the same alleged violations by Defendant Newcourse, and the same unreasonable manner of notifying individuals about the Data Breach.

110. **Adequacy**. Plaintiffs will fairly and adequately protect the proposed Class's interests. Plaintiffs' interests do not conflict with Class members' interests, and Plaintiffs have

retained counsel experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf, including as lead counsel. Defendant has no defenses unique to Plaintiffs.

111. **Commonality**. Plaintiffs' and the Class's claims raise predominantly common fact and legal questions that a class wide proceeding can answer for all Class members. Common questions for the Class include, but are not necessarily limited to the following:

a. Whether Defendants had a duty to use reasonable care in safeguarding the PII of Plaintiffs, and the Class;

b. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether FUB failed to ensure Newcourse implemented and maintained reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

d. Whether Defendants were negligent in maintaining, protecting, and securing PII;

e. Whether Defendants breached their contractual promises to safeguard the Plaintiffs' and the Class's PII;

f. Whether Defendants took reasonable measures to determine the extent of the Data Breach after discovering it;

g. Whether Defendants' Data Breach Notice(s) was/were reasonable;

h. Whether Defendants' conduct was likely to deceive the public;

i. Whether Defendants are liable for negligence or gross negligence;

j. Whether Defendants' practices and representations related to the Data Breach breached implied warranties;

k. Whether the Data Breach caused Plaintiffs and the Class injuries;

l. What the proper damages measure is; and

m. Whether Plaintiffs and the Class are entitled to damages, or declaratory or injunctive relief.

112. Further, this action satisfies Tenn. R. Civ. P. 23.02 because: (i) common questions of law and fact predominate over any individualized questions; (ii) prosecuting individual actions would create a risk of inconsistent or varying adjudications, risking incompatible standards of conduct for Defendant, and a risk of adjudications with respect to individual members of the Class which would as a practical matter be dispositive of the interests of the other members not parties to the adjudications or would substantially impair or impede their ability to protect their interest; and (iii) the Defendant has acted or refused to act on grounds generally applicable to the Class, thereby making appropriate final injunctive relief or corresponding declaratory relief with respect to the Class as a whole.

COUNT I,
NEGLIGENCE

113. Plaintiffs and members of the Class incorporate all previous paragraphs as if fully set forth herein.

114. Defendants were entrusted with the private, sensitive personal information, PII, of Plaintiffs and the proposed Class Members, received from their financial and other institutions, including FUB, as a condition of receiving services.

115. Defendants owed to Plaintiffs and members of the Class a duty to exercise reasonable care in handling and using the PII in its care and custody, including implementing

industry-standard security procedures sufficient to reasonably protect the information from the Data Breach, theft, and unauthorized use that came to pass, and to promptly detect attempts at unauthorized access. Further, FUB owed Plaintiffs and members of the Class a duty to ensure its vendor, Newcourse, exercised reasonable care in handling and using the PII in its care and custody.

116. Defendants owed a duty of care to Plaintiffs and members of the Class because it was foreseeable that Defendant's failure to adequately safeguard the PII in accordance with state-of-the-art industry standards concerning data security would result in the compromise of that PII—just like the Data Breach that ultimately came to pass. Defendant acted with wanton and reckless disregard for the security and confidentiality of the PII of Plaintiffs and members of the Class by disclosing and providing access to this information to third parties and by failing to properly supervise both the way the PII was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

117. Defendants owed to Plaintiffs and members of the Class a duty to notify them within a reasonable timeframe of any breach to the security of the PII. Defendant also owed a duty to timely and accurately disclose to Plaintiffs and members of the Class the scope, nature, and occurrence of the Data Breach. This duty is required and necessary for Plaintiffs and members of the Class to take appropriate measures to protect the PII, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

118. Defendants owed these duties to Plaintiffs and members of the Class because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendants knew or should have known would suffer injury-in-fact from Defendants' inadequate security protocols. Defendants actively sought and obtained Plaintiffs' and members of the Class's personal information and PII.

119. The risk that unauthorized persons would attempt to gain access to the PII and misuse it was foreseeable. Given that Defendants hold vast amounts of PII, it was inevitable that unauthorized individuals would attempt to access Defendant's databases containing the PII—whether by a hacking attack or otherwise.

120. PII is highly valuable, and Defendants knew, or should have known, the risk in obtaining, using, handling, emailing, and storing of the PII of Plaintiffs and members of the Class, and the importance of exercising reasonable care in handling it.

121. Newcourse breached its duties by failing to exercise reasonable care in handling and securing the personal information and PII of Plaintiffs and members of the Class which actually and proximately caused the Data Breach and Plaintiffs' and members of the Class's injury. Newcourse further breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiffs and members of the Class, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiffs' and members of the Class's injuries-in-fact.

122. FUB breached its duties by failing to exercise reasonable care in supervising its agents, contractors, vendors, and suppliers, including Newcourse, and in handling and securing the personal information and PII of Plaintiffs and members of the Class which actually and proximately caused the Data Breach and Plaintiffs' and members of the Class's injury. FUB further breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiffs and members of the Class, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiffs' and members of the Class's injuries-in-fact.

123. As a direct and traceable result of Defendants' negligence and/or negligent supervision, Plaintiffs and members of the Class have suffered or will imminently suffer damages,

including fraudulent activity and identity theft, monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

124. Defendants' breach of their common-law duties to exercise reasonable care and their failures and negligence actually and proximately caused Plaintiffs and members of the Class actual, tangible, injury-in-fact and damages, including, without limitation, fraudulent activity and identity theft, imminent harm resulting from fraudulent activity using Plaintiffs' and the Class Members' PII unauthorizedly disclosed by Defendants; the loss of the opportunity to control how their PII is used; diminution in value of their PII; the compromise, publication and/or theft of their PII; out-of-pocket costs associated with the prevention, detection, recovery and remediation from identity theft or fraud, including the purchase of identity theft protection insurance and detection services; lost opportunity costs and lost wages associated with the time and effort expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from identity theft and fraud; delay in receipt of tax refund monies; unauthorized use of stolen PII; continued risk to their PII, which remains in the possession of Defendants and is subject to further breaches so long as they fail to undertake appropriate measures to protect the PII in their possession; and current and future costs related to the time, effort, and money that will be expended to prevent, detect, contest, remediate and repair the impact of the Data Breach for the remainder of the lives of Plaintiffs and Class members, all entitling them to damages in an amount to be proven at trial.

COUNT II,
NEGLIGENCE *PER SE*

125. Plaintiffs and members of the Class incorporate all previous paragraphs as if fully set forth herein.

126. 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 the PII of Plaintiffs and members of the Class. This is in addition to Defendants' common law duties owed to Plaintiffs and the Class Members set forth in the preceding paragraphs.

127. 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 or, in this case, patients' PII. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendants' duty to protect the PII of Plaintiffs and members of the Class.

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

129. 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 Plaintiffs and members of the Class.

130. Defendants had a duty to Plaintiffs and the members of the Class to implement and maintain reasonable security procedures and practices to safeguard the PII of Plaintiffs and members of the Class.

131. Further, FUB had a duty to Plaintiffs and the members of the Class to ensure that its vendor, Newcourse, implement and maintain reasonable security procedures and practices to safeguard their PII.

132. Defendants breached their respective duties to Plaintiffs and members of the Class pursuant to the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard the PII of Plaintiffs and members of the Class, and by FUB failing to ensure that Newcourse undertook such measures.

133. Defendants' violation of Section 5 of the FTC Act and its failure to comply with applicable laws and regulations constitutes negligence per se.

134. But for Defendants' wrongful and negligent breach of their duties owed to Plaintiffs and members of the Class, Plaintiffs and members of the Class would not have been injured.

135. The injury and harm suffered by Plaintiffs and members of the Class were the reasonably foreseeable result of Defendants' breach of their duties. Defendants knew or should have known that they, including Newcourse, was failing to meet its duties and that its breach would cause Plaintiffs and members of the Class to suffer the foreseeable harms associated with the exposure of their PII.

136. Had Plaintiffs and members of the Class known that Defendants did not adequately protect their PII, or ensure vendors protected their PII, Plaintiffs and members of the Class would not have entrusted FUB with their PII or permitted that PII to be retained by Newcourse.

137. Defendants' negligence *per se* actually and proximately caused Plaintiffs and members of the Class actual, tangible, injury-in-fact and damages, including, without limitation, imminent harm resulting from fraudulent activity using Plaintiffs' and the Class Members' PII unauthorizedly disclosed by Defendants; the loss of the opportunity to control how their PII is

used; diminution in value of their PII; the compromise, publication and/or theft of their PII; out-of-pocket costs associated with the prevention, detection, recovery and remediation from identity theft or fraud, including the purchase of identity theft protection insurance and detection services; lost opportunity costs and lost wages associated with the time and effort expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from identity theft and fraud; delay in receipt of tax refund monies; unauthorized use of stolen PII; continued risk to their PII, which remains in the possession of Defendants and is subject to further breaches so long as they fail to undertake appropriate measures to protect the PII in their possession; and current and future costs related to the time, effort, and money that will be expended to prevent, detect, contest, remediate and repair the impact of the Data Breach for the remainder of the lives of Plaintiffs and Class members, all entitling them to damages in an amount to be proven at trial.

COUNT III,
INVASION OF PRIVACY—INTRUSION UPON SECLUSION

138. Plaintiffs and members of the Class incorporate all previous paragraphs as if fully set forth herein.

139. Plaintiffs and the proposed Class Members had a legitimate expectation of privacy regarding their highly private, confidential, PII—including their names, Social Security Numbers, and other information—and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

140. Defendants owed a duty to its customers, including Plaintiff and the Class, to keep the above-described private information, PII, confidential.

141. The access by an unauthorized party of Plaintiffs' and Class Members' PHI is

highly offensive to a reasonable person.

142. The intrusion was into a place or thing which was private and entitled to be private. Plaintiff and the Class disclosed their sensitive and confidential PII to financial and other institutions, including but not limited to FUB, which was then entrusted to Newcourse as part of Defendants' services, but did so privately, with the intention that their information would be kept confidential and protected from unauthorized disclosure. Plaintiffs and the Class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

143. In the Data Breach, Newcourse intentionally publicly disclosed the private facts of the Plaintiffs and the Class.

144. Further, the Data Breach constitutes an intentional interference with Plaintiffs' and the Class's interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

145. Defendants acted with a knowing state of mind when they permitted the Data Breach because they knew its information security practices, or FUB knew that Newcourse's security practices, were inadequate.

146. Further, Defendants acted with a knowing state of mind when it failed to notify Plaintiffs and the Class in a timely fashion about the Data Breach, thereby materially impairing their mitigation efforts.

147. Acting with knowledge, Defendants had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiffs and the Class.

148. As a proximate result of Defendants' acts and omissions, the private and sensitive PII of Plaintiffs and the Class were unauthorizedly accessed, and upon information and belief, are

now public and available to disclosure and redisclosure without authorization, causing Plaintiffs and the Class to suffer injury and damages as alleged herein.

COUNT IV,
BREACH OF IMPLIED CONTRACT

149. Plaintiffs and members of the Class incorporate all previous paragraphs as if fully set forth herein.

150. FUB offered to provide financial services to Plaintiffs, and members of the Class, in exchange for their PII and in exchange for amounts paid for services that included payment for data security. FUB provided this PII to its third-party vendor, Newcourse, in connection with Defendants providing financial services to Plaintiffs and the Class Members.

151. In turn, by their conduct, and through internal policies, Defendants each agreed they would not disclose the PII collected to unauthorized persons. FUB also promised to safeguard customer PII, including to protect Plaintiffs' and the Class Members' PII with security measures that comply with federal law including computer safeguards, secured files and buildings, and other safeguards.[45]

152. Plaintiffs and the members of the Class accepted Defendants' offer by providing PII in exchange for financial services, including those mailing services rendered by Newcourse.

153. Implicit in the parties' agreement was that Defendants would provide Plaintiffs and members of the Class with prompt and adequate notice of all unauthorized access and/or theft of their PII.

154. Plaintiffs and the members of the Class would not have entrusted their PII to Defendants in the absence of such agreement.

[45] See First United Bank, Consumer Privacy Policy, available at https://www.firstunitedbank.com/privacy-policy.

155. Defendants each materially breached the contract(s) it had entered with Plaintiffs and members of the Class by failing to safeguard such information, PII, including by FUB failing to ensure its third-party vendor, Newcourse, undertook adequate data security measures, and failing to notify them promptly of the intrusion into its computer systems that compromised such information. FUB further breached the implied contracts with Plaintiffs and members of the Class by:

a. Failing to properly safeguard and protect the PII of Plaintiffs and members of the Class;

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 electronic PII that Defendants created, received, maintained, and transmitted.

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

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

158. 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.

159. 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.

160. Defendants failed to advise Plaintiffs and members of the Class of the Data Breach promptly and sufficiently.

161. In these and other ways, Defendants violated their duties of good faith and fair dealing.

162. Plaintiffs 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 V,
THIRD-PARTY BENEFICIARY

163. Plaintiffs and members of the Class incorporate all previous paragraphs as if fully set forth herein.

164. Plaintiffs and the proposed Class Members are the third-party beneficiaries of a contract between Newcourse and Plaintiffs' and the Class's financial and other institutions, under which Newcourse: received Plaintiffs and the Class Members' personal information, PII, stored that information, and provided printing services to their institutions.

165. Plaintiffs allege that Defendants have breached the contract by failing to adequately safeguard that PII in the Data Breach.

166. Defendants each materially breached the contract(s) it had entered with Plaintiffs and members of the Class by failing to safeguard such information, PII, including by FUB failing to ensure its third-party vendor, Newcourse, undertook adequate data security measures, and failing to notify them promptly of the intrusion into its computer systems that compromised such

information.

167. Plaintiffs 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 VI,
UNJUST ENRICHMENT

168. Plaintiffs and members of the Class incorporate all previous paragraphs as if fully set forth herein.

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

170. Plaintiffs and members of the Class conferred a benefit upon Defendants, FUB and Newcourse, in the form of monies paid for financial services and by providing their PII, in order to receive financial services.

171. Defendants appreciated or had knowledge of the benefits conferred upon itself by Plaintiffs and members of the Class.

172. As a result of Defendants' conduct, Plaintiffs and members of the Class suffered actual damages in an amount equal to the difference in value between the purchases made with reasonable data privacy and security practices and procedures that Plaintiffs and members of the Class paid for, and the purchases without unreasonable data privacy and security practices and procedures that they received.

173. Under principals of equity and good conscience, Defendants should not be permitted to retain the full value of Plaintiffs' and the proposed Class's payments and their PII because Defendant failed to adequately protect their PII. Plaintiffs and the proposed Class would not have provided their PII, nor used and paid for FUB's services, had they known FUB would not

adequately protect their PII and ensure its vendor, Newcourse, adequately protected PII.

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

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, JOSIAH AREND, and BREANNA AREND, individually and on behalf of all others similarly situated, the proposed Class Members, demand a 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 Plaintiffs and the proposed Class, appointing Plaintiffs as class representative, and appointing their counsel to represent the Class;

B. Awarding Plaintiffs and the Class damages that include applicable compensatory, exemplary, punitive damages, restitution, and statutory damages, as allowed by law, in an amount to be determined at trial;

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

D. Awarding injunctive relief as is necessary to protect the interests of Plaintiffs and the Class;

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

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

G. Granting Plaintiffs and the Class leave to amend this complaint to conform to the evidence produced at trial; and

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

EFILED 02/08/23 06:33 AM CASE NO. 23C303 Joseph P. Day, Clerk

JURY DEMAND

Plaintiffs demand a trial by jury on all issues so triable.

February 8, 2023

Respectfully submitted,

/s/ J. Gerard Stranch, IV
J. Gerard Stranch IV (BPR 23045)
Andrew E. Mize*
BRANSTETTER STRANCH & JENNINGS, PLLC
The Freedom Center
223 Rosa L. Parks Avenue, Suite 200
Nashville, Tennessee 27203
(615) 254-8801
gerards@bsjfirm.com
andrewm@bsjfirm.com

Lynn A. Toops*
Amina A. Thomas*
COHEN & MALAD, LLP
One Indiana Square, Suite 1400
Indianapolis, Indiana 46204
(317) 636-6481
ltoops@cohenandmalad.com
athomas@cohenandmalad.com

Matthew D. Alison, OBA No. 32723
INDIAN & ENVIRONMENTAL LAW GROUP, PLLC
406 South Boulder Avenue, Suite 830
Tulsa, Oklahoma 74103
(918) 347-6169
(918) 948-6190 (facsimile)
matthew@iaelaw.com

Counsel for the Plaintiffs, Josiah Arend, and Breanna Arend, and the Proposed Class

*Motion for *Pro Hac Vice* forthcoming