IN THE UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF MISSOURI

WALEED LASHIN, individually and on behalf of all others similarly situated, Plaintiff, v. **T-MOBILE US, INC.,** Defendant.	Case No. **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Waleed Lashin ("Dr. Lashin" or "Plaintiff"), individually and on behalf of all others similarly situated, brings this action against T-Mobile US, Inc. ("Defendant" or "T-Mobile"). The following allegations are based on Plaintiff's knowledge, investigations of counsel, facts of public record, and information and belief.

NATURE OF THE ACTION

1. Plaintiff seeks to hold Defendant responsible for the injuries Defendant inflicted on Plaintiff and approximately 836[1] similarly situated persons ("Class Members") due to Defendant's impermissibly inadequate data security, which caused the personal information of Plaintiff and those similarly situated to be exfiltrated by unauthorized access by cybercriminals (the "Data Breach" or "Breach") between February 24, 2023, to March 30, 2023.[2]

[1] https://apps.web.maine.gov/online/aeviewer/ME/40/ea3bf342-eca7-4833-b128-7b09f6893ac4.shtml (last accessed June 1, 2023).
[2] *Id.*

2. The data that Defendant caused to be exfiltrated by cybercriminals for the purpose of engaging identity theft to the detriment and injury to Plaintiff and Class Members were highly sensitive. Upon information and belief, the exfiltrated data included personal identifying information ("PII"), including individuals' full name, contact information, account number and associated phone numbers, T-Mobile account PIN, social security number, government ID, date of birth, balance due, internal codes that T-Mobile uses to service customer accounts (for example, rate plan and feature codes), and the number of lines.[3]

3. Upon information and belief, prior to and through the date of the Data Breach, Defendant obtained Plaintiff's and Class Members' PII and then maintained that sensitive data in a negligent and/or reckless manner. As evidenced by the Data Breach, Defendant inadequately maintained their network, platform, software, and technology partners—rendering these easy prey for cybercriminals.

4. Upon information and belief, the risk of the Data Breach was known to Defendant. Thus, Defendant were on notice that their inadequate data security created a heightened risk of exfiltration, compromise, and theft.

5. Then, after the Data Breach, Defendant failed to provide timely notice to the affected Plaintiff and Class Members—thereby exacerbating their injuries. Ultimately, Defendant deprived Plaintiff and Class Members of the chance to take speedy measures to protect themselves and mitigate harm. Simply put, Defendant impermissibly left Plaintiff

[3] https://apps.web.maine.gov/online/aeviewer/ME/40/ea3bf342-eca7-4833-b128-7b09f6893ac4/00363120-37a5-4248-aa8c-0be84d146071/document.html.

and Class Members in the dark—thereby causing their injuries to fester and the damage to spread.

6. Even when Defendant finally notified Plaintiff and Class Members of their PII's exfiltration, Defendant failed to adequately describe the Data Breach and its effects.

7. Today, the identities of Plaintiff and Class Members have been compromised—all because of Defendant's negligence. Plaintiff and Class Members now suffer from a present and continuing risk of harm, including fraud and identity theft, and must now constantly monitor their financial accounts.

8. Armed with the PII stolen in the Data Breach, criminals can commit a litany of crimes. Specifically, criminals can now open new financial accounts in Class Members' names, take out loans using Class Members' identities, use Class Members' identities to obtain government benefits, file fraudulent tax returns using Class Members' information, obtain driver's licenses in Class Members' names (but with another person's photograph), and give false information to police during an arrest.

9. And Plaintiff and Class Members will and have suffered additional financial costs for purchasing necessary credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

10. Plaintiff and Class Members have suffered—and will continue to suffer—from the loss of the benefit of their bargain, unexpected out-of-pocket expenses, lost or diminished value of their PII, emotional distress, and the value of their time reasonably incurred to mitigate the fallout of the Data Breach.

11. Through this action, Plaintiff seeks to remedy these injuries on behalf of themselves and all similarly situated individuals whose PII were exfiltrated and compromised in the Data Breach.

12. Plaintiff seeks remedies including, but not limited to, compensatory damages, treble damages, punitive damages, reimbursement of out-of-pocket costs, and injunctive relief—including improvements to Defendant's data security systems, future annual audits, and adequate credit monitoring services funded by Defendant.

PARTIES

13. Plaintiff Waleed Lashin is a natural person and resident and citizen of the State of New Jersey. Dr. Lashin has no intention of moving to a different state in the immediate future.

14. Defendant T-Mobile US, Inc. is a Delaware corporation with its principal place of business in Bellevue, Washington.

JURISDICTION AND VENUE

15. This Court has original jurisdiction under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2), because this is a class action involving more than 100 putative class members and the amount in controversy exceeds $5,000,000, exclusive of interest and costs. And minimal diversity is established because Plaintiff and many members of the class are citizens of states different than that of Defendant.

16. This Court has general personal jurisdiction over Defendant because Defendant is authorized to conduct business in this State and has intentionally availed itself

of the laws and markets within this State conducting substantial business in this State. Defendant sells, markets, and advertises its products and services to Plaintiffs and Class Members located in the State of California and, therefore, has sufficient minimum contacts to render the exercise of jurisdiction by this Court proper and necessary.

17. Venue is proper in this District under 28 U.S.C. §§ 1391(a)(2), 1391(b)(2), and 1391(c)(2) because substantial part of the events giving rise to the claims emanated from activities within this District, and Defendant conducts substantial business in this District.

FACTUAL ALLEGATIONS

Defendant Collected and Stored the PII of Plaintiff and Class Members

18. Defendant is a telecommunications company that provides wireless voice, messaging, and data services along with mobile phones and accessories.

19. Defendant operates its business nationwide offering various types of technological products and services.

20. Upon information and belief, Defendant received and maintained the PII of Plaintiff and Class Members.

21. Plaintiff and the Class Members, as current or former T-Mobile users, reasonably relied (directly or indirectly) on this sophisticated technology company to keep their sensitive PII confidential; to maintain its system security; to use this information for business purposes only; and to make only authorized disclosures of their PII. Borrowers,

in general, demand security to safeguard their PII, especially when financial information and other sensitive PII is involved.

22. Because of the highly sensitive and personal nature of the information Defendant acquire and store, Defendant knew or reasonably should have known that it stored protected PII and must comply with federal and state laws protecting customers' PII, and provide adequate notice to customers if their PII is disclosed without proper authorization.

23. When Defendant collects this sensitive information, it promises to use reasonable measures to safeguard the PII from theft and misuse.

24. Defendant acquired, collected, and stored, and represented that it maintained reasonable security over Plaintiff's and Class Members' PII.

25. By obtaining, collecting, receiving, and/or storing Plaintiff's and Class Members' PII, Defendant assumed legal and equitable duties and knew, or should have known, that it was thereafter responsible for protecting Plaintiff's and Class Members' PII from unauthorized disclosure.

26. Upon information and belief, Defendant promises to only share Plaintiff's and Class Members' PII in limited circumstances, none of which include sharing such information with hackers.

27. Upon information and belief, Defendant represented to its customers in written contracts, marketing materials, and otherwise that it would properly protect all PII it obtained.

28. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII, including but not limited to, protecting their usernames and passwords, using only strong passwords for their accounts, and refraining from browsing potentially unsafe websites.

29. Upon information and belief, Plaintiff and Class Members relied on Defendant to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

30. Defendant could have prevented or mitigated the effects of the Data Breach by better securing its network, properly encrypting its data, or better selecting and supervising its information technology partners.

31. Defendant's negligence in safeguarding Plaintiff's and Class Members' PII was exacerbated by repeated warnings and alerts directed to protecting and securing sensitive data, as evidenced by the trending data breach attacks in recent years. In 2022, the damages from identity theft has been projected to reach $8 trillion dollars. https://www.juniperresearch.com/press/cybercrime-to-cost-global-business-over-8-trn

32. Despite the prevalence of public announcements of data breaches and data security compromises making it readily apparent to anyone, including Defendant, in possession of sensitive and valuable personally identifiable information that it was not a matter of if they would be susceptible to a security incident which might result in a data breach, but when. Defendant failed to take appropriate steps to protect Plaintiff's and Class Members' PII from being compromised.

33. Defendant failed to properly select their information security partners.

34. Defendant failed to ensure the proper monitoring and logging of the ingress and egress of network traffic.

35. Defendant failed to ensure the proper monitoring and logging of file access and modifications.

36. Defendant failed to ensure the proper training of their employees and their technology partners' employees as to cybersecurity best practices.

37. Defendant failed to ensure fair, reasonable, or adequate computer systems and data security practices to safeguard the PII of Plaintiff and Class Members.

38. Defendant failed to timely and accurately disclose that Plaintiff's and Class Members' PII had been improperly acquired or accessed.

39. Defendant knowingly disregarded standard information security principles, despite obvious risks, by allowing unmonitored and unrestricted access to unsecured PII.

40. Defendant failed to provide adequate supervision and oversight of the PII with which it was and is entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted an unknown third party to gather PII of Plaintiff and Class Members, misuse the PHI/PII and potentially disclose it to others without consent.

41. Upon information and belief, Defendant failed to ensure the proper implementation of sufficient processes to quickly detect and respond to data breaches, security incidents, or intrusions.

42. Upon information and belief, Defendant failed to ensure the proper encryption of Plaintiff's and Class Members' PII and monitor user behavior and activity to identify possible threats.

The Data Breach

43. On or about April 28 of 2023, Defendant notified the public ("Notice of Data Breach" or "Notice") that its customers' data had been compromised in a Data Breach, and informed them of the following:

> Our systems recently detected that a bad actor accessed limited information from a small number of T-Mobile accounts, including your T-Mobile account PIN. Personal financial account information and call records were NOT affected. Our systems and policies enabled T-Mobile teams to identify the activity, terminate it, and implement measures to protect against it from occurring again in the future. To further protect your account, we have already proactively reset your PIN.
>
> While we have a number of safeguards in place to prevent unauthorized access such as this from happening, we recognize that we must continue to make improvements to stay ahead of bad actors. We take these issues seriously. We apologize that this happened and are furthering efforts to enhance security of your information.
>
> **What Happened?**
>
> In March 2023, the measures we have in place to alert us to unauthorized activity worked as designed and we were able to determine that a bad actor gained access to limited information from a small number of T-Mobile accounts between late February and March 2023.
>
> **What Information Was Involved?**
>
> No personal financial account information or call records were affected. The information obtained for each customer varied, but may have included full name, contact information, account number and associated phone numbers, T-Mobile account PIN, social security number, government ID, date of birth, balance due, internal codes that T-Mobile uses to service customer accounts (for example, rate plan and feature codes), and the number of lines.[4]

[4] https://apps.web.maine.gov/online/aeviewer/ME/40/ea3bf342-eca7-4833-b128-7b09f6893ac4/00363120-37a5-4248-aa8c-0be84d146071/document.html.

44. Although the Data Breach began on February 24, 2023, it was not until March 27, 2023—over a month later—that Defendant became aware of suspicious activity on their network.

45. Although the Data Breach was discovered on March 27, 2023, it was not until March 30, 2023—three days later—that Defendant was able to stop the intrusion.

46. Although the Data Breach was discovered on March 27, 2023, it was not until April 28, 2023—over a month later—that Defendant notified the public.

47. Upon information and belief, Plaintiff's and Class Members' PII was access, exfiltrated, and stolen in the Breach.

48. Upon information and belief, Plaintiff's and Class Members' affected PII was accessible, unencrypted, unprotected, and vulnerable for acquisition and/or exfiltration by unauthorized individuals.

49. Time is of the essence when highly sensitive PII is subject to unauthorized access and/or acquisition. The disclosed, accessed, and/or acquired PII of Plaintiff and Class Members is likely available on the Dark Web. Hackers can access and then offer for sale the unencrypted, unredacted PII to criminals. Plaintiff and Class Members are now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from the possible publication of their PII onto the Dark Web. Plaintiff and Class Members now face a lifetime risk of identity theft, which is heightened here by unauthorized access, disclosure, and/or activity by cybercriminals on computer systems containing sensitive personal information.

50. Following the Breach and recognizing that each Class Member is now subject to the present and continuing risk of identity theft and fraud, Defendant advised impacted individuals to "remain vigilant by monitoring account activity and free credit reports, and reviewing your security choices on your email, financial, and other accounts."[5] Defendant also advised Plaintiff and Class Members to "place a fraud alert with the three major credit bureaus which we have listed below. A fraud alert lets creditors know to contact you before opening new accounts in your name. You can call any one of the three credit bureaus at the number below to place a fraud alert on your credit file without charge, and they will contact the other two bureaus on your behalf. Additionally, some states allow residents to place a no-cost 'freeze' on their credit file with the credit bureau."[6]

51. Defendant largely put the burden on Plaintiff and Class Members to take measures to protect themselves.

52. Time is a compensable and valuable resource in the United States. According to the U.S. Bureau of Labor Statistics, 55.5% of U.S.-based workers are compensated on an hourly basis, while the other 44.5% are salaried.[7]

---

[5] https://apps.web.maine.gov/online/aeviewer/ME/40/ea3bf342-eca7-4833-b128-7b09f6893ac4/00363120-37a5-4248-aa8c-0be84d146071/document.html.

[6] *Id.*

[7] *Characteristics of minimum wage workers, 2020*, U.S. BUREAU OF LABOR STATISTICS https://www.bls.gov/opub/reports/minimum-wage/2020/home.htm#:~:text=In%202020%2C%2073.3%20million%20workers,wage%20of%20%247.25%20per%20hour (last accessed Oct. 21, 2022); *Average Weekly Wage Data*, U.S. BUREAU OF LABOR STATISTICS, *Average Weekly Wage Data,* https://data.bls.gov/cew/apps/table_maker/v4/table_maker.htm%23type=1&year=2021&qtr=3&own=5&ind=10&supp=0 (last accessed Aug. 2, 2022) (finding that on average, private-sector workers make $1,253 per 40-hour work week.).

53. According to the U.S. Bureau of Labor Statistics' 2018 American Time Use Survey, American adults have only 36 to 40 hours of "leisure time" outside of work per week;[8] leisure time is defined as time not occupied with work or chores and is "the time equivalent of 'disposable income.'"[9] Usually, this time can be spent at the option and choice of the consumer, however, having been notified of the Data Breach, consumers now have to spend hours of their leisure time self-monitoring their accounts, communicating with financial institutions and government entities, and placing other prophylactic measures in place to attempt to protect themselves.

54. Plaintiff and Class Members are now deprived of the choice as to how to spend their valuable free hours and seek renumeration for the loss of valuable time as another element of damages.

55. Upon information and belief, the unauthorized third-party cybercriminals gained access to Plaintiff's and Class Members' PII with the intent of engaging in misuse of the PII, including marketing and selling Plaintiff's and Class Members' PII.

56. Defendant also offered credit monitoring services to some Class Members for a period of 24 months. Such measures, however, are insufficient to protect Plaintiff and Class Members from the lifetime risks they each now face. As another element of damages, Plaintiff and Class Members seek a sum of money sufficient to provide Plaintiff and Class Members identity theft protection services for their respective lifetimes.

---

[8] Cory Stieg, *You're spending your free time wrong — here's what to do to be happier and more successful*, CNBC https://www.cnbc.com/2019/11/06/how-successful-people-spend-leisure-time-james-wallman.html (Nov. 6, 2019).
[9] *Id.*

57. Defendant's Breach Notice letter, as well as its website notice, both omit the size and scope of the breach. Defendant have demonstrated a pattern of providing inadequate notices and disclosures about the Data Breach.

58. Plaintiff and the Class Members remain, even today, in the dark regarding what particular data was stolen, the particular ransomware used, and what steps are being taken, if any, to secure their PII and financial information going forward. Plaintiff and Class Members are left to speculate as to the full impact of the Data Breach and how exactly Defendant intends to enhance its information security systems and monitoring capabilities so as to prevent further breaches.

59. Plaintiff's and Class Members' PII and financial information may end up for sale on the dark web, or simply fall into the hands of companies that will use the detailed PII and financial information for targeted marketing without the approval of Plaintiff and/or Class Members. Either way, unauthorized individuals can now easily access the PII and/or financial information of Plaintiff and Class Members.

Defendant Failed to Comply with FTC Guidelines

60. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making.[10] To that end, the FTC has issued numerous guidelines identifying best data security practices that businesses, such as Defendant, should employ to protect against the unlawful exfiltration of PII.

[10] *Start with Security: A Guide for Business*, FED. TRADE COMM'N (June 2015), https://bit.ly/3uSoYWF (last accessed July 25, 2022).

61. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[11] The guidelines explain that businesses should:

a. protect the personal customer information that they keep;

b. properly dispose of personal information that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

62. The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

63. The FTC recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[12]

64. 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

[11] *Protecting Personal Information: A Guide for Business*, FED. TRADE COMM'N (Oct. 2016), https://bit.ly/3u9mzre (last accessed July 25, 2022).
[12] *See Start with Security*, *supra* note 46.

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.

65. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to customer PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

Defendant Failed to Follow Industry Standards

66. Despite its alleged commitments to securing sensitive PII, Defendant does not follow industry standard practices in securing PII.

67. Several best practices have been identified that at a minimum should be implemented by Defendant, including but not limited to, educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

68. Other best cybersecurity practices that are standard include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

69. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation

PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

70. Such frameworks are the existing and applicable industry standards and Defendant failed to comply with these accepted standards, thus opening the door to criminals and the Data Breach.

The Experiences and Injuries of Plaintiff and Class Members

71. Plaintiff and Class Members are current or former T-Mobile subscribers.

72. As a prerequisite of receiving Defendant's services, Defendant requires its customers to provide their PII to Defendant.

73. When Defendant finally announced the Data Breach, it deliberately underplayed the Breach's severity and obfuscated the nature of the Breach. Defendant's Breach Notice sent to Plaintiff and Class Members fails to explain how the breach occurred (what security weakness was exploited), what exact data elements of each affected individual were compromised, who the Breach was perpetrated by, and the extent to which those data elements were compromised.

74. Because of the Data Breach, Defendant inflicted injuries upon Plaintiff and Class Members. And yet, Defendant have done little to provide Plaintiff and the Class Members with relief for the damages they suffered.

75. All Class Members were injured when Defendant caused their PII to be exfiltrated by cybercriminals.

76. Plaintiff and Class Members entrusted their PII to Defendant. Thus, Plaintiff had the reasonable expectation and understanding that Defendant would take—*at minimum*—industry standard precautions to protect, maintain, and safeguard that information from unauthorized users or disclosure, and would timely notify them of any data security incidents. After all, Plaintiff would not have entrusted their PII to any entity that used Defendant's services had they known that Defendant would not take reasonable steps to safeguard their information.

77. Plaintiff and Class Members suffered actual injury from having their PII compromised in the Data Breach including, but not limited to, (a) damage to and diminution in the value of their PII—a form of property that Defendant obtained from Plaintiff; (b) violation of their privacy rights; (c) the likely theft of their PII; (d) fraudulent activity resulting from the Breach; and (e) present and continuing injury arising from the increased risk of additional identity theft and fraud.

78. As a result of the Data Breach, Plaintiff and Class Members also suffered emotional distress because of the release of their PII—which they believed would be protected from unauthorized access and disclosure. Now, Plaintiff suffer from anxiety about unauthorized parties viewing, selling, and/or using their PII for nefarious purposes like identity theft and fraud.

79. Plaintiff and Class Members also suffer anxiety about unauthorized parties viewing, using, and/or publishing their information related to their medical records and prescriptions.

80. Because of the Data Breach, Plaintiff and Class Members have spent—and will continue to spend—considerable time and money to try to mitigate and address harms caused by the Data Breach.

Plaintiff Lashin's Experience

81. Dr. Lashin opened a T-Mobile cellular phone business account for himself, his wife, and other members of his family, for a total of five cellular phone lines, beginning in 2016 until approximately April 2, 2023 ("T-Mobile Account").

82. Dr. Lashin used one of the cellular phone lines associated with his T-Mobile Account to communicate with his patients, though the use of (1) after hour pages including patients name, date of birth, symptoms, and phone numbers and (2) multiple HIPAA compliant health care practice application suites, which include, access to complete hospital medical records, note dictation through voice recognition, and access to patient charts. Dr. Lashin regularly used these features in the ordinary course of providing healthcare services to his patients.

83. At all relevant times, Dr. Lashin took reasonable measures to protect his PII and online presence, including using Google Authenticator two-factor authentication when using his phone to make financial transactions.

84. Plaintiff received a Notice of Data Breach letter from Defendant on or about the beginning of May of 2023.

85. Shortly after and as a result of the Data Breach, Plaintiff Lashin experienced a large increase in spam and suspicious phone calls, texts, and emails.

86. During and as a result of the Data Breach, Dr. Lashin received a two-factor authentication text message from PayPal for a login not made or authorized by him.

87. During the late afternoon of February 28, 2023, Dr. Lashin's iPhone went into "SOS" mode, and he discovered that his T-Mobile enabled phone lost cellular service. At or around 6:00 P.M that day, Dr. Lashin also received an email message from T-Mobile stating that he had cancelled his internet account.

88. Approximately one hour later following what he believed to be a T-Mobile cellular service outage, Dr. Lashin began receiving email notifications that the cryptocurrency he was maintaining in his Coinbase account was being converted into Bitcoin, and that cash was being transferred out of his Coinbase account. At no time did Dr. Lashin authorize the February 28, 2023 conversions to Bitcoin or the cash transfers out of his Coinbase account. Dr. Lashin came to the conclusion that his T-Mobile account had been compromised. The total value of the cash and cryptocurrency loss experienced by Dr. Lashin is approximately $13,000.

89. Immediately following his receipt of the Coinbase email notifications on February 28, 2023, Dr. Lashin called the 611 T-Mobile support line, and spent about an hour speaking with T-Mobile. Dr. Lashin was ultimately successful in recovering ownership of his T-Mobile cellular account after being charged $15 by T-Mobile for a new eSim.

90. During that call with the 611 T-Mobile support line, Dr. Lashin was told numerous times in telephone discussions with T-Mobile representatives that the service outage and loss of cellular service was due to a "system glitch".

91. During that call with the 611 T-Mobile support line, T-Mobile falsely represented to Dr. Lashin that the loss of cellular service was due to a "system glitch" when in fact it was due to a T-Mobile system compromise.

92. During that call with the 611 T-Mobile support line, a T-Mobile representative informed Dr. Lashin that a prepaid phone line was added to his T-Mobile account. At no time did Dr. Lashin cause or authorize a prepaid phone line to be added to his T-Mobile cellular account. Dr. Lashin later learned in a subsequent call that an unidentified person had contacted Defendant T-Mobile to open that prepaid phone line. Later that day, Dr. Lashin obtained a one-time PIN to log into and retook ownership of his T-Mobile Account. On March 3, 2023, when Dr. Lashin called T-Mobile back and demanded to know exactly what happened, T-Mobile eventually informed Dr. Lashin that a onetime PIN was issued on February 28, 2023, shortly before his phone was hacked.

93. Dr. Lashin's T-Mobile phone stored various passwords to other applications, and, not surprisingly, his Microsoft Hotmail account was also compromised following the Data Breach.

94. On March 1, 2023, Dr. Lashin reported the incident to local law enforcement, and was advised to and did report the incidents to the Passaic County White Collar Crime division.

95. On or about March 11, 2023, Dr. Lashin's wife contacted him and told him that her T-Mobile cellular phone had lost cellular coverage and went into "SOS" mode. Dr. Lashin's wife immediately called the 611 number. T-Mobile opened a ticket, and Dr. Lashin's wife was provided with a new eSim and her number was recovered within two

hours.

96. During mid-March, 2023, Dr. Lashin learned from a T-Mobile phone representative that a second attempt was made to add another pre-paid phone line to his T-Mobile account.

97. On March 31, 2023, Dr. Lashin's wife received a text notification that the T-Mobile PIN number associated with the account had been changed. However; T-Mobile told Dr. Lashin's wife not to worry, and that she received this message to remind her to establish a PIN for herself. This did not make sense since the message from T-Mobile notified her that the account PIN was changed. This change was the result of fraudulent activity and not initiated by an authorized user.

98. Following the March 31, 2023 compromise, Dr. Lashin switched carriers, spending nearly a full day away from his medical practice to obtain the release of the numbers associated with his T-Mobile Account.

99. On May 4, 2023, Dr. Lashin received a Notice of Data Breach letter from T-Mobile.

100. Although Dr. Lashin and his wife have obtained and paid for numerous identity protection programs (the costs of which were reasonable and necessary), the Lashins remain concerned that the financial loss, and emotional toll resulting from the Data Breach will continue.

101. Dr. Lashin has spent significant time responding to the Data Breach and will continue to spend valuable time he otherwise would have spent on other activities, including but not limited to work and/or recreation.

102. Dr. Lashin suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has experienced anxiety and increased concerns for the loss of his privacy, as well as anxiety over the impact of cybercriminals accessing and using his PII and/or financial information.

103. Dr. Lashin is now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from his PII and financial information, in combination with his name, being placed in the hands of unauthorized third parties/criminals.

104. Dr. Lashin has a continuing interest in ensuring that his PII and financial information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff and the Proposed Class Face Significant Risk of Present and Continuing Identity Theft

105. Plaintiff and Class Members suffered injury from the misuse of their PII that can be directly traced to Defendant.

106. The ramifications of Defendant's failure to keep Plaintiff's and the Class's PII secure are severe. Identity theft occurs when someone uses another's personal and financial information such as that person's name, account number, Social Security number, driver's license number, date of birth, and/or other information, without permission, to commit fraud or other crimes.

107. According to experts, one out of four data breach notification recipients become a victim of identity fraud.[13]

108. As a result of Defendant's failures to prevent—and to timely detect—the Data Breach, Plaintiff and Class Members suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at an increased risk of suffering:

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

b. The diminution in value of their PII;

c. The compromise and continuing publication of their PII;

d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

e. Lost opportunity costs and lost wages associated with the time and effort expended 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;

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen PII; and

[13] *More Than 12 Million Identity Fraud Victims in 2012 According to Latest Javelin Strategy & Research Report*, BUSINESSWIRE (Feb. 20, 2013) https://threatpost.com/study-shows-one-four-who-receive-data-breach-letter-become-fraud-victims-022013/77549/.

h. The continued risk to their PII, which remains in the possession of Defendant and is subject to further breaches so long as Defendant fails to undertake the appropriate measures to protect the PII in their possession.

109. Stolen PII is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII can be worth up to $1,000.00 depending on the type of information obtained.[14]

110. The value of Plaintiff's and the proposed Class's PII on the black market is considerable. Stolen PII trades on the black market for years, and criminals frequently post stolen private information openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

111. It can take victims years to spot or identify PII theft, giving criminals plenty of time to milk that information for cash.

112. One such example of criminals using PII for profit is the development of "Fullz" packages.[15]

---

[14] Brian Stack, *Here's How Much Your Personal Information Is Selling for on the Dark Web*, EXPERIAN (Dec. 6, 2017) https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/.

[15] "Fullz" is fraudster-speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money can be made off those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record or more on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz", which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See, e.g.*, Brian Krebs, *Medical Records For Sale in Underground*

113. Cyber-criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

114. 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 cyber-criminals 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.

115. 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, resulting in more than $3.5 billion in losses to individuals and business victims.

Stolen From Texas Life Insurance Firm, KREBS ON SECURITY, (Sep. 18, 2014) https://krebsonsecurity.com/tag/fullz/.

116. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good." Defendant did not rapidly report to Plaintiff and the Class that their PII had been stolen.

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

118. In addition to out-of-pocket expenses that can exceed thousands of dollars and the emotional toll identity theft can take, some victims have to 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 continuously monitor their reports for future inaccuracies, close existing bank/credit accounts, open new ones, and dispute charges with creditors.

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

120. 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."[16]

121. The FTC has also issued numerous guidelines for businesses that highlight the importance of reasonable data security practices. The FTC has noted the need to factor data security into all business decision-making.[17] 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.[18]

122. 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.[19] The FTC treats the failure to employ reasonable and

[16] *Commissioner Pamela Jones Harbour: Remarks Before FTC Exploring Privacy Roundtable*, FED. TRADE COMMISSION (Dec. 7, 2009), https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-ftc-exploring-privacy-roundtable/091207privacyroundtable.pdf.

[17] *Start With Security, A Guide for Business*, FED. TRADE COMMISSION, https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited Oct. 21, 2022).

[18] *Id.*

[19] *See Taking Charge, What to Do If Your Identity is Stolen*, FED. TRADE COMMISSION, at 3 (2012), https://www.ojp.gov/ncjrs/virtual-library/abstracts/taking-charge-what-do-if-your-identity-stolen.

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 (the "FTCA").

123. To that end, the FTC has issued orders against businesses that failed to employ reasonable measures to secure sensitive payment card data. *See In the matter of Lookout Services, Inc.*, No. C-4326, ¶ 7 (June 15, 2011) ("[Defendant] allowed users to bypass authentication procedures" and "failed to employ sufficient measures to detect and prevent unauthorized access to computer networks, such as employing an intrusion detection system and monitoring system logs."); *In the matter of DSW, Inc.*, No. C-4157, ¶ 7 (Mar. 7, 2006) ("[Defendant] failed to employ sufficient measures to detect unauthorized access."); *In the matter of The TJX Cos., Inc.*, No. C-4227 (Jul. 29, 2008) ("[R]espondent stored . . . personal information obtained to verify checks and process unreceipted returns in clear text on its in-store and corporate networks[,]" "did not require network administrators . . . to use different passwords to access different programs, computers, and networks[,]" and "failed to employ sufficient measures to detect and prevent unauthorized access to computer networks . . ."); *In the matter of Dave & Buster's Inc.*, No. C-4291 (May 20, 2010) ("[Defendant] failed to monitor and filter outbound traffic from its networks to identify and block export of sensitive personal information without authorization" and "failed to use readily available security measures to limit access between instore networks . . ."). These orders, which all preceded the Data Breach, further clarify the measures businesses must take to meet their data security obligations. Defendant thus knew or should have known that its data security protocols were inadequate and were likely to result in the unauthorized access to and/or theft of PII.

124. Defendant disclosed the PII of Plaintiff and members of the proposed Class for criminals to use in the conduct of criminal activity. Specifically, Defendant opened, disclosed, and failed to adequately protect the PII of Plaintiff and members of the proposed Class to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen PII.

125. Defendant's use of outdated and insecure computer systems and software that are easy to hack, and its failure to maintain adequate security measures and an up-to-date technology security strategy, demonstrates a willful and conscious disregard for privacy, and has failed to adequately protect the PII of Plaintiff and potentially thousands of members of the proposed Class to unscrupulous operators, con artists, and outright criminals.

126. Defendant's failure to properly notify Plaintiff and members of the proposed Class of the Data Breach exacerbated Plaintiff's and members of the proposed Class's injury by depriving them of the earliest ability to take appropriate measures to protect their PII and take other necessary steps to mitigate the harm caused by the Data Breach.

CLASS ACTION ALLEGATIONS

127. Plaintiff brings this action individually and on behalf of all other persons similarly situated ("the Class") under Fed. R. Civ. P. 23(b)(2), 23(b)(3), and 23(c)(4).

128. Plaintiff proposes the following Class definitions, subject to amendment as appropriate:

> All persons residing in the United States whose PII or PHI was impacted by the Data Breach—including all persons that received a Notice of the Data Breach (the "Class").

129. The Class defined above is readily ascertainable from information in Defendant's possession. Thus, such identification of Class Members will be reliable and administratively feasible.

130. Excluded from the Class are: (1) any judge or magistrate presiding over this action and members of their families; (2) Defendant and its subsidiaries, parents, successors, predecessors, affiliated entities, and any entity in which their parents have 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) Plaintiff's counsel and Defendant's counsel; (6) members of the jury; and (7) the legal representatives, successors, and assigns of any such excluded persons.

131. Plaintiff reserves the right to amend or modify the Class definition—including potential Subclasses—as this case progresses.

132. Plaintiff and Class Members satisfy the numerosity, commonality, typicality, and adequacy requirements under Fed. R. Civ. P. 23.

133. **Numerosity**. The Class Members are numerous such that joinder is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time, based on information and belief, the Class consists of the approximately 836 individuals whose PII were compromised by Defendant's Data Breach.

134. **Commonality**. There are many questions of law and fact common to the Class. And these common questions predominate over any individualized questions of individual Class Members. These common questions of law and fact include, without limitation:

a. If Defendant unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' PII;

b. If Defendant 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. If Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations including;

d. If Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

e. If Defendant owed a duty to Class Members to safeguard their PII;

f. If Defendant breached its duty to Class Members to safeguard their PII;

g. If Defendant knew or should have known that its data security systems and monitoring processes were deficient;

h. If Defendant should have discovered the Data Breach earlier;

i. If Defendant took reasonable measures to determine the extent of the Data Breach after it was discovered;

j. If Defendant's delay in informing Plaintiff and Class Members of the Data Breach was unreasonable;

k. If Defendant's method of informing Plaintiff and Class Members of the Data Breach was unreasonable;

l. If Defendant's conduct was negligent;

m. If Plaintiff and Class Members were injured as a proximate cause or result of the Data Breach;

n. If Plaintiff and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

o. If Defendant breached implied contracts with Plaintiff and Class Members;

p. If Defendant was unjustly enriched by unlawfully retaining a benefit conferred upon them by Plaintiff and Class Members;

q. If Defendant failed to provide notice of the Data Breach in a timely manner; and

r. If Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages, treble damages, and/or injunctive relief.

135. **Typicality**. Plaintiff's claims are typical of those of other Class Members because Plaintiff's information, like that of every other Class Member, was compromised in the Data Breach. Moreover, all Plaintiff and Class Members were subjected to Defendant's uniformly illegal and impermissible conduct.

136. **Adequacy of Representation**. Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff's Counsel are competent and experienced in litigating complex class actions. Plaintiff has no interests that conflict with, or are antagonistic to, those of the Class.

137. **Predominance**. Defendant has engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff and Class Members' data was stored on the same network system and unlawfully and inadequately protected in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

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

139. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable

identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

140. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

141. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include those set forth above.

142. Defendant has acted on grounds that apply generally to the Class as a whole, so that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

FIRST CAUSE OF ACTION
Negligence
(On Behalf of Plaintiff and the Class)

143. Plaintiff re-alleges and incorporate by reference paragraphs 1-142 of the Complaint as if fully set forth herein.

144. Defendant required its customers to submit Plaintiff's and Class Members' non-public PII to receive Defendant's services.

145. By collecting and storing this data in their computer system and network, and sharing it and using it for commercial gain, Defendant owed a duty of care to use reasonable means to secure and safeguard their computer system—and Plaintiff's and Class Members' PII held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes

so they could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

146. The risk that unauthorized persons would attempt to gain access to the PII and misuse it was foreseeable. Given that Defendant holds vast amounts of PII, it was inevitable that unauthorized individuals would at some point try to access Defendant's databases of PII.

147. After all, PII is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the PII of Plaintiff and Class Members. Thus, Defendant knew, or should have known, the importance of exercising reasonable care in handling the PII entrusted to them.

148. Defendant owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that their systems and networks, and the personnel responsible for them, adequately protected the PII.

149. Defendant's duty of care to use reasonable security measures arose because of the special relationship that existed between Defendant and Plaintiff and Class Members, which is recognized by laws and regulations, as well as common law. Defendant were in a superior position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

150. Defendant failed to take appropriate measures to protect the PII of Plaintiff and the Class. Any purported safeguards that Defendant had in place were wholly inadequate.

151. Defendant breached its duty to exercise reasonable care in safeguarding and protecting Plaintiff's and the Class members' PII by failing to adopt, implement, and maintain adequate security measures to safeguard that information, despite known data breaches, and allowing unauthorized access to Plaintiff's and the other Class Members' PII.

152. The failure of Defendant to comply with industry and federal regulations evinces Defendant's negligence in failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' PII.

153. But for Defendant's wrongful and negligent breach of their duties to Plaintiff and the Classes, members' PII would not have been compromised, stolen, and viewed by unauthorized persons. Defendant's negligence was a direct and legal cause of the theft of the PII of Plaintiff and the Classes and all resulting damages.

154. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendant's failure to exercise reasonable care in safeguarding and protecting Plaintiff's and the other Class members' PII. Defendant knew or should have known that their systems and technologies for processing and securing the PII of Plaintiff and the Classes had security vulnerabilities.

155. As a result of this misconduct by Defendant, the PII, PHI, and other sensitive information of Plaintiff and the Classes was compromised, placing them at a greater risk of identity theft and their PII being disclosed to third parties without the consent of Plaintiff and the Classes

SECOND CAUSE OF ACTION
Negligence *Per Se*
(On Behalf of Plaintiff and the Class)

156. Plaintiff re-alleges and incorporate by reference paragraphs 1-141 of the Complaint as if fully set forth herein.

157. Under the Federal Trade Commission Act, Defendant had a duty to employ reasonable security measures. Specifically, this statute prohibits "unfair . . . practices in or affecting commerce," including (as interpreted and enforced by the FTC) the unfair practice of failing to use reasonable measures to protect confidential data.[20]

158. Moreover, Plaintiff and Class Members' injuries are precisely the type of injuries that the FTCA guards against. After all, 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 very same injuries that Defendant inflicted upon Plaintiff and Class Members.

159. Defendant's duty to use reasonable care in protecting confidential data arose not only because of the statutes and regulations described above, but also because Defendant are bound by industry standards to protect confidential PII.

160. Defendant owed Plaintiff and Class Members a duty to notify them within a reasonable time frame of any breach to their PII. Defendant also owed a duty to timely and accurately disclose to Plaintiff and Class Members the scope, nature, and occurrence of the Data Breach. This duty is necessary for Plaintiff and Class Members to take appropriate

[20] 15 U.S.C. § 45.

measures to protect their PII, to be vigilant in the face of an increased risk of harm, and to take other necessary steps in an effort to mitigate the fallout of Defendant's Data Breach.

161. Defendant owed these duties to Plaintiff and Class Members because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from its inadequate security protocols. After all, Defendant actively sought and obtained the PII of Plaintiff and Class Members.

162. Defendant breached their duties, and thus were negligent, by failing to use reasonable measures to protect Plaintiff's and Class Members' PII. And but for Defendant's negligence, Plaintiff and Class Members would not have been injured. The specific negligent acts and omissions committed by Defendant include, but are not limited to:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' PII;

b. Failing to comply with—and thus violating—FTCA and its regulations;

c. Failing to adequately monitor the security of its networks and systems;

d. Failing to have in place mitigation policies and procedures;

e. Allowing unauthorized access to Class Members' PII;

f. Failing to detect in a timely manner that Class Members' PII had been compromised; and

g. Failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

163. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' PII would result in injury to Class Members. It was therefore foreseeable that the failure to adequately safeguard Class Members' PII would result in one or more types of injuries to Class Members.

164. Simply put, Defendant's negligence actually and proximately caused Plaintiff and Class Members actual, tangible, injuries-in-fact and damages. These injuries include, but are not limited to, the theft of their PII by criminals, improper disclosure of their PII, lost benefit of their bargain, lost value of their PII, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendant's negligence. Moreover, injuries-in-fact and damages are ongoing, imminent, and immediate.

165. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered because of the Data Breach.

166. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, *e.g.,* (1) strengthen their data security systems and monitoring procedures; (2) submit to future annual audits of those systems and monitoring procedures; and (3) continue to provide adequate credit monitoring to all Class Members for the remainders of their lives.

THIRD CAUSE OF ACTION
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

167. Plaintiff re-alleges and incorporate by reference paragraphs 1-142 of the Complaint as if fully set forth herein.

168. This cause of action is plead in the alternative to the breach of implied contract theory.

169. Plaintiff and Class Members conferred a monetary benefit on Defendant, by paying money for services that relied on Defendant to render certain services, a portion of which was intended to have been used by Defendant for data security measures to secure Plaintiff and Class Members' PII. Plaintiff and Class Members further conferred a benefit on Defendant by entrusting their PII to Defendant from which Defendant derived profits.

170. Defendant enriched themselves by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class Members' PII. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to avoid their data security obligations at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide adequate security.

171. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

172. Defendant acquired the monetary benefit, PII, and PHI through inequitable means in that Defendant failed to disclose the inadequate security practices, previously alleged, and failed to maintain adequate data security.

173. If Plaintiff and Class Members knew that Defendant had not secured their PII, they would not have agreed to give their money—or disclosed their data—to Defendant or Defendant's customers.

174. Plaintiff and Class Members have no adequate remedy at law.

175. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered—and will continue to suffer—a host of injuries, including but not limited to: (1) actual identity theft; (2) the loss of the opportunity to determine how their PII is used; (3) the compromise, publication, and/or theft of their PII; (4) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII; (5) lost opportunity costs associated with effort expended and the loss of productivity 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; (6) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in their possession; and (7) future expenditures of time, effort, and money that will be spent trying to prevent, detect, contest, and repair the impact of Defendant's Data Breach.

176. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members suffered—and will continue to suffer—other forms of injury and/or harm.

177. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from Plaintiff and Class Members.

FOURTH CAUSE OF ACTION
Breach of Implied Contract
(On Behalf of Plaintiff and the Class)

178. Plaintiff re-alleges and incorporate by reference paragraphs 1-142 of the Complaint as if fully set forth herein.

179. Defendant required Plaintiff and the Class to provide and entrust their PII/PHI and financial information as a condition of obtaining services from Defendant.

180. Plaintiff and the Class paid money to Defendant in exchange for goods and services, as well as Defendant's promises to protect their PII from unauthorized disclosure.

181. Defendant promised to make sure that Plaintiff's and Class Members' PII would remain protected.

182. Through its course of conduct, Defendant, Plaintiff, and Class Members entered into implied contracts for Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiff's and Class Members' PHI and PII and financial information.

183. Defendant solicited and invited Plaintiff and Class Members to provide their PHI/PII and financial information as part of Defendant's regular business practices.

Plaintiff and Class Members accepted Defendant's offers and provided their PHI/PII and financial information to Defendant.

184. As a condition of being direct customers of Defendant, Plaintiff and Class Members provided and entrusted their PHI/PII and financial information to Defendant. In so doing, Plaintiff and Class Members entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such non-public information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and Class Members if its data had been breached and compromised or stolen.

185. A meeting of the minds occurred when Plaintiff and Class Members agreed to, and did, provide its PHI/PII and financial information to Defendant, in exchange for, amongst other things, the protection of its PHI/PII and financial information.

186. Plaintiff and Class Members fully performed their obligations under the implied contracts with Defendant.

187. Defendant breached the implied contracts it made with Plaintiff and Class Members by failing to safeguard and protect their PHI/PII and financial information and by failing to provide timely and accurate notice to them that their PHI/PII and financial information was compromised as a result of the Data Breach.

188. Defendant further breached the implied contracts with Plaintiff and Class Members by failing to ensure the confidentiality and integrity of PII Defendant created, received, maintained, and transmitted in violation of 45 CFR 164.306(a)(1).

189. Defendant further breached the implied contracts with Plaintiff and Class Members by failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 CFR 164.308(a)(1).

190. Defendant further breached the implied contracts with Plaintiff and Class Members by failing to protect against any reasonably anticipated threats or hazards to the security or integrity of PII in violation of 45 CFR 164.306(a)(2).

191. Defendant's failures to meet these promises constitute breaches of the implied contracts.

192. Furthermore, the failure to meet its confidentiality and privacy obligations resulted in Defendant providing goods and services to Plaintiff and Class Members that were of a diminished value.

193. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and Class Members have suffered (and will continue to suffer) (a) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; (b) actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; (c) loss of the confidentiality of the stolen confidential data; (d) the illegal sale of the compromised data on the dark web; (e) lost work time; and (f) other economic and non-economic harm.

194. As a result of Defendant's breach of implied contract, Plaintiff and the Class Members are entitled to and demand actual, consequential, and nominal damages.

PRAYER FOR RELIEF

WHEREFORE Plaintiff, individually and on behalf of all others similarly situated, requests the following relief:

A. An Order certifying this action as a class action and appointing Plaintiff as Class representative and the undersigned as Class counsel;

B. A mandatory injunction directing Defendant to adequately safeguard the PII of Plaintiff and the Class hereinafter by implementing improved security procedures and measures, including but not limited to an Order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendant to delete and purge the PII of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of Plaintiff's and Class Members' PII;

v. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring, simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis;

vi. prohibiting Defendant from maintaining Plaintiff's and Class Members' PII on a cloud-based database until proper safeguards and processes are implemented;

vii. requiring Defendant to segment data by creating firewalls and access controls so that, if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

viii. requiring Defendant to conduct regular database scanning and securing checks;

ix. requiring Defendant to monitor ingress and egress of all network traffic;

x. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling PII, as well as protecting the PII of Plaintiff and Class Members;

xi. requiring Defendant to implement a system of tests to assess their respective employees' knowledge of the education programs

discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

xii. requiring Defendant to implement, maintain, review, and revise as necessary a threat management program to appropriately monitor Defendant's networks for internal and external threats, and assess whether monitoring tools are properly configured, tested, and updated; and

xiii. requiring Defendant to meaningfully educate all Class Members about the threats that they face because of the loss of its confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves.

C. A mandatory injunction requiring that Defendant provide notice to each member of the Class relating to the full nature and extent of the Data Breach and the disclosure of PII to unauthorized persons;

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

E. An award of damages, including actual, nominal, consequential damages, and punitive, as allowed by law in an amount to be determined;

F. An award of attorneys' fees, costs, and litigation expenses, as allowed by law;

G. An award of pre- and post-judgment interest, costs, attorneys' fees, expenses, and interest as permitted by law;

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

I. For all other Orders, findings, and determinations identified and sought in this Complaint; and

J. Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

Under Federal Rule of Civil Procedure 38(b), Plaintiff demands a trial by jury for any and all issues in this action so triable as of right.

Dated: June 8, 2023

Respectfully Submitted,

/s/ Alexander A. Wolff

John A. Yanchunis*
JYanchunis@forthepeople.com
Marcio W. Valladares*
MValladares@forthepeople.com
Ra O. Amen*
RAmen@forthepeople.com
MORGAN & MORGAN
COMPLEX LITIGATION GROUP
201 North Franklin Street 7th Floor
Tampa, Florida 33602
T: (813) 223-5505
F: (813) 223-5402

Alexander A. Wolff
Missouri Bar No. 64247
AWolff@forthepeople.com
MORGAN & MORGAN
200 N. Broadway Suite 720
St. Louis, MO 63102
T: (314) 955-1045
F: (314) 955-1069

Steven W. Teppler*
steppler@mblawfirm.com
MANDELBAUM BARRET, P.C.
3 Becker Farm Road, Suite 105
Roseland, NJ 07068
T: (646) 946-5659
F: (973) 325-7467

Counsel for Plaintiff and the Class
**Pro hac vice forthcoming*

ClassAction.org