# Exhibit A

**UNITED STATES DISTRICT COURT**
**FOR THE NORTHERN DISTRICT OF ILLINOIS**
**EASTERN DIVISON**

| | |
|---|---|
| TONY GOODRUM and JASON MIXON, individually and on behalf of all others similarly situated,<br><br>Plaintiffs,<br><br>v.<br><br>VERADIGM, INC.,<br><br>Defendant. | **Case No.: 1:25-cv-07062**<br><br>**AMENDED CONSOLIDATED CLASS ACTION COMPLAINT**<br><br>Honorable John Robert Blakey<br><br>**JURY TRIAL DEMANDED** |

Plaintiffs Tony Goodrum, Marty Wooley, Todd Clay, and Tanya Walker ("Plaintiffs"), individually, and on behalf of all others similarly situated, by and through their undersigned counsel, bring this Amended Consolidated Class Action Complaint against Veradigm, Inc. ("Defendant"). Plaintiffs allege the following upon information and belief based on the investigation of counsel, except as to those allegations that specifically pertain to Plaintiffs, which are alleged upon personal knowledge.

## INTRODUCTION

1. Plaintiffs and the proposed Class Members bring this class action lawsuit on behalf of all persons who entrusted Defendant with sensitive Personally Identifiable Information ("PII")[1] and Protected Health Information ("PHI") (collectively, "Private Information") that was impacted in a data breach (the "Data Breach" or the "Breach").

[1] Personally identifiable information generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual.

2. Plaintiffs' claims arise from Defendant's failure to properly secure and safeguard Private Information that was entrusted to it and its accompanying responsibility to store and transfer that information.

3. This is a "hub-and-spoke" data breach, where Defendant, the "hub," processes and maintains data for numerous clients, the "spokes."

4. Defendant is a healthcare technology company that uses data and analytics to improve healthcare delivery for various clients, including Urology Associates of Mobile, P.A., Neighborhood Health Center of WNY, Inc., Family Medical Group of Texarkana, LLP, Peachtree Neurological Clinic, P.C., Virginia Ear, Nose & Throat Associates, P.C., Cabarrus Eye Center, P.A., and North Buncombe Family Medicine, P.A. (hereinafter, the "Clients" or "Defendant's Clients").

5. Defendant had numerous statutory, regulatory, contractual, and common law duties and obligations, including those based on affirmative representations to Plaintiffs and Class Members, to keep their Private Information confidential, safe, secure, and protected from unauthorized disclosure or access.

6. Upon information and belief, on or around December of 2024, Defendant experienced a cyber incident on a server used to store data of Clients' patients and policyholders. As a result of the Data Breach, an unauthorized third-party was able to access and copy files containing the sensitive Private Information of Plaintiffs and Class Members.

7. Upon information and belief, the following types of Private Information were compromised in the Data Breach: name, Social Security number, phone number, and medical information.

8. It is believed that the notorious ransomware group Rhysida was responsible for the Data Breach.

9. Defendant failed to take precautions designed to keep individuals' Private Information secure.

10. Defendant owed Plaintiffs and Class Members a duty to take all reasonable and necessary measures to keep the Private Information collected safe and secure from unauthorized access. Defendant solicited, collected, used, and derived a benefit from the Private Information, yet breached its duty by failing to implement or maintain adequate security practices.

11. The Private Information compromised in the Data Breach contained highly sensitive patient data, representing a gold mine for data thieves. The data included, but is not limited to, Social Security numbers and sensitive medical information that Defendant collected and maintained on behalf of its Clients' patients and policyholders.

12. Armed with the Private Information accessed in the Data Breach (and a head start), data thieves can commit a variety of crimes including, *e.g.*, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' names to obtain medical services, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, and giving false information to police during an arrest.

13. There has been no acknowledgement yet by Defendant that the Data Breach occurred nor any assurances that Defendant is taking steps to protect the Private Information going forward.

14. Therefore, Plaintiffs and Class Members have suffered and are at an imminent, immediate, and continuing increased risk of suffering, ascertainable losses in the form of harm

from identity theft and other fraudulent misuse of their Private Information, the loss of the benefit of their bargain, out-of-pocket expenses incurred to remedy or mitigate the effects of the Data Breach, and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach.

15. Plaintiffs bring this class action lawsuit to address Defendant's inadequate safeguarding of Class Members' Private Information that it collected and maintained on behalf of its Clients, and its failure to provide timely and adequate notice to its Clients and their affected patients, including Plaintiffs and Class Members, of the Breach and the types of information unlawfully accessed.

16. The potential for improper disclosure and theft of Plaintiffs and Class Members' Private Information was a known risk to Defendant, and thus Defendant was on notice that failing to take necessary steps to secure the Private Information left it vulnerable to an attack.

17. Upon information and belief, Defendant failed to properly monitor and implement security practices with regard to the computer network and systems that housed the Private Information. Had Defendant properly monitored its IT Network, it would have discovered the Breach sooner.

18. Plaintiffs and Class Members' identities are now at risk because of Defendant's negligent conduct as the Private Information that Defendant collected and maintained on behalf of its Clients is now in the hands of data thieves and other unauthorized third parties.

19. Plaintiffs seek to remedy these harms on behalf of themselves and all similarly situated individuals whose Private Information was accessed and/or compromised during the Data Breach.

20. Accordingly, Plaintiffs, on behalf of themselves and the Class, assert claims for negligence, negligence *per se*, breach of third-party beneficiary contract, unjust enrichment, and declaratory judgment.

## PARTIES

***Plaintiffs***

21. Plaintiff Tony Goodrum is a citizen and resident of Waveland, Mississippi.

22. Plaintiff Marty Wooley is a citizen and resident of Semmes, Alabama.

23. Plaintiff Todd Clay is a citizen and resident of Mount Pleasant, North Carolina.

24. Plaintiff Tanya Walker is a citizen and resident of Mars Hill, North Carolina.

***Defendant***

25. Defendant is a corporation organized under the state laws of Delaware with its principal place of business located at 222 Merchandise Mart Plz, Ste 2024, Chicago, Illinois, 60654. Defendant's registered agent is CT Corporation System, located at 208 S. Lasalle Street, Suite 814, Chicago, Illinois, 60604.

## JURISDICTION AND VENUE

26. This Court has jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. The number of class members is more than 100 and at least one member of the Class defined below is a citizen of a different state that is diverse from Defendant's citizenship. Thus, minimal diversity exists under 28 U.S.C. § 1332 (d) (2) (A). Defendant has its principal place of business located in this District.

27. This Court has personal jurisdiction over Defendant because Defendant is registered to do business and maintains its principal place of business in this District.

28. Venue is proper in this Court because Defendant's principal place of business is located in this District, and because a substantial part of the events, acts, and omissions giving rise to Plaintiffs' claims occurred in this District.

## FACTUAL ALLEGATIONS

### A. Background on Defendant

29. Defendant is a healthcare technology company that uses data and analytics to improve healthcare delivery for various clients, including life sciences companies, health plans, and healthcare providers. Formerly known as Allscripts Healthcare Solutions, Defendant rebranded to its current name in January 2023.

30. As a condition of doing business, Defendant requires that Clients entrust it with highly sensitive personal information belonging to their patients and policyholders. In the ordinary course of receiving service from Defendant's Clients, Plaintiffs and Class Members were required to provide their Private Information to Defendant.

31. Upon information and belief, Defendant made promises and representations to individuals', including Plaintiffs and Class Members, that the Private Information collected from them would be kept safe and confidential, and that the privacy of that information would be maintained.

32. Plaintiffs and Class Members provided their Private Information to Defendant with the reasonable expectation and on the mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

33. As a result of collecting and storing the Private Information of Plaintiffs and Class Members for its own financial benefit, Defendant had a continuous duty to adopt and employ

reasonable measures to protect Plaintiffs and the Class Members' Private Information from disclosure to third parties.

**B. The Data Breach**

34. On or around December of 2024, upon information and belief, Defendant's IT Network was infiltrated by cybercriminals. As a result of the Data Breach, the unauthorized third-party was able to access and copy files on Defendant's IT Network containing Private Information of Defendant's Clients patients and policyholders.

35. Upon information and belief, the following types of Private Information were compromised in the Data Breach: name, Social Security number, phone number, and medical information.

36. The ransomware group Rhysida is believed to be responsible for the Data Breach. Rhysida is a ransomware group that encrypts data on victims' computer systems and threatens to make it publicly available unless a ransom is paid. The group uses eponymous ransomware-as-a-service techniques, targets large organizations rather than making random attacks on individuals, and demands large sums of money to restore data.

37. The group takes its name from the Rhysida genus of centipedes, which analysts have speculated is meant to project an image of stealth and shadows.[2]

38. Defendant had obligations created by the FTC Act, HIPPA, contract, common law, and industry standards to keep Plaintiffs and Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

[2] https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-rhysida (last visited August 21, 2025).

39. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information they were maintaining for Plaintiffs and Class Members, causing the exposure of Private Information, such as encrypting the information or deleting it when it is no longer needed.

40. The Data Breach resulted in unauthorized third-party accessing and acquiring files containing unencrypted Private Information of Plaintiffs and Class Members. Plaintiffs and Class Members' Private Information was accessed and stolen in the Data Breach.

41. Upon information and belief, Plaintiffs' Private Information, and that of Class Members, was subsequently published on the dark web following the Data Breach, as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type.

42. Defendant failed to take precautions designed to keep individuals' Private Information secure.

43. Individuals affected by the Data Breach are, and remain, at risk that their data will be sold or listed on the dark web and, ultimately, illegally used in the future.

**C. Defendant's Failure to Prevent, Identify, and Timely Report the Data Breach**

44. Defendant failed to take adequate measures to protect its computer systems against unauthorized access.

45. The Private Information that Defendant allowed to be exposed in the Data Breach is the type of private information that Defendant knew or should have known would be the target of cyberattacks.

46. Despite its own knowledge of the inherent risks of cyberattacks, and

notwithstanding the FTC's data security principles and practices,[3] Defendant failed to disclose that its systems and security practices were inadequate to reasonably safeguard its past and present clients or customers Private Information.

47. The FTC directs businesses to use an intrusion detection system to expose a breach as soon as it occurs, monitor activity for attempted hacks, and have an immediate response plan if a breach occurs.[4] Immediate notification of a Data Breach is critical so that those impacted can take measures to protect themselves.

48. Defendant has yet to acknowledge to the Data Breach, let alone, inform individuals' impacted by it.

**D. The Harm Caused by the Data Breach Now and Going Forward**

49. Victims of data breaches are susceptible to becoming victims of identity theft. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 17 C.F.R. § 248.201(9). When "identity thieves have your personal information, they can drain your bank account, run up charges on your credit cards, open new utility accounts, or get medical treatment on your health insurance."[5]

50. The type of data that may have been accessed and compromised here can be used to perpetrate fraud and identity theft.

51. Plaintiffs and Class Members face a substantial risk of identity theft given that their Private Information was compromised in the Data Breach.

---

[3] *Protecting Personal Information: A Guide for Business,* FED. TRADE COMM'N (Oct. 2016), https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business. (last visited August 21, 2025).

[4] *Id.*

[5] *Prevention and Preparedness*, New York State Police, https://troopers.ny.gov/prevention-and-preparedness (last visited August 21, 2025).

52. Stolen Private Information is often trafficked on the "dark web," a heavily encrypted part of the Internet that is not accessible via traditional search engines. Law enforcement has difficulty policing the "dark web" due to this encryption, which allows users and criminals to conceal their identities and online activity.

53. When malicious actors infiltrate companies and copy and exfiltrate the Private Information that those companies store, the stolen information often ends up on the dark web where malicious actors buy and sell that information for profit.[6]

54. For example, when the U.S. Department of Justice announced their seizure of AlphaBay—the largest online "dark market"—in 2017, AlphaBay had more than 350,000 listings, many of which concerned stolen or fraudulent documents that could be used to assume another person's identity."[7] Marketplaces similar to the now-defunct AlphaBay continue to be "awash with [PII] belonging to victims from countries all over the world."[8]

55. PII remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[9] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[10]

---

[6] *Shining a Light on the Dark Web with Identity Monitoring*, IDENTITYFORCE (Dec. 28, 2020) https://www.identityforce.com/blog/shining-light-dark-web-identity-monitoring (last visited August 21, 2025).
[7] *Stolen PII & Ramifications: Identity Theft and Fraud on the Dark Web*, ARMOR (April 3, 2018), https://res.armor.com/resources/blog/stolen-pii-ramifications-identity-theft-fraud-dark-web/ (last visited August 21, 2025).
[8] *Id.*
[9] *Id.*
[10] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015) https://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited August 21, 2025).

56. 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 in 2019, resulting in more than $3.5 billion in losses to individuals and business victims.[11]

57. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good."[12] Defendant did not rapidly report to Plaintiffs and Class Members that their Private Information had been stolen. Defendant has yet to notify impacted people of the Data Breach.

58. As a result of the Data Breach, the Private Information of Plaintiffs and Class Members has been exposed to criminals for misuse. The injuries suffered by Plaintiffs and Class Members, or likely to be suffered as a direct result of Defendant's Data Breach, include: (a) theft of their Private Information; (b) costs associated with the detection and prevention of identity theft; (c) costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the consequences of this Breach; (d) invasion of privacy; (e) the emotional distress, stress, nuisance, and annoyance of responding to, and resulting from, the Data Breach; (f) the actual and/or imminent injury arising from actual and/or potential fraud and identity theft resulting from their personal data being placed in the hands of the ill-intentioned hackers and/or criminals; (g) damage to and diminution in value of their personal data entrusted to Defendant with the mutual understanding that Defendant would safeguard their Private Information against theft and not allow access to and misuse of their personal data by any unauthorized third party; and (h) the continued risk to their Private

[11] *2019 Internet Crime Report Released*, FBI (Feb. 11, 2020) https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120#:~:text=IC3%20received%20467%2C361%20complaints%20in,%2Ddelivery%20scams%2C%20and%20extortion (last visited August 21, 2025).
[12] *Id.*

Information, which remains in the possession of Defendant, and which is subject to further injurious breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs and Class Members' Private Information.

59. In addition to a remedy for economic harm, Plaintiffs and Class Members maintain an interest in ensuring that their Private Information is secure, remains secure, and is not subject to further misappropriation and theft.

60. Defendant disregarded the rights of Plaintiffs and Class Members by (a) intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure that its network servers were protected against unauthorized intrusions; (b) failing to disclose that it did not have adequately robust security protocols and training practices in place to safeguard Plaintiffs and Class Members' Private Information; (c) failing to take standard and reasonably available steps to prevent the Data Breach; (d) concealing the existence and extent of the Data Breach for an unreasonable duration of time; and (e) failing to provide Plaintiffs and Class Members prompt and accurate notice of the Data Breach.

61. The actual and adverse effects to Plaintiffs and Class Members, including the imminent, immediate, and continuing increased risk of harm for identity theft, identity fraud and/or medical fraud directly or proximately caused by Defendant's wrongful actions and/or inaction and the resulting Data Breach require Plaintiffs and Class Members to take affirmative acts to recover their peace of mind and personal security including, without limitation, purchasing credit reporting services, purchasing credit monitoring and/or internet monitoring services, frequently obtaining, purchasing and reviewing credit reports, bank statements, and other similar information, instituting and/or removing credit freezes and/or closing or modifying financial accounts, for which there is a financial and temporal cost. Plaintiffs and other Class Members

have suffered, and will continue to suffer, such damages for the foreseeable future.

***Plaintiff Tony Goodrum's Experience***

62. Plaintiff Goodrum is a former patient of Defendant's Client, Urology Associates of Mobile, P.A..

63. As a condition of obtaining medical services, Plaintiff Goodrum was required to provide Defendant and its Client with his Private Information—including name, Social Security number, date of birth, and contact information.

64. Defendant was in possession of Plaintiff Goodrum's Private Information before, during, and after the Data Breach.

65. Plaintiff Goodrum reasonably understood and expected that Defendant would safeguard his Private Information and timely and adequately notify him in the event of a data breach. Plaintiff Goodrum would not have allowed Defendant, or anyone in Defendant's position, to maintain his Private Information if he believed that Defendant would fail to implement reasonable and industry standard practices to safeguard that information from unauthorized access.

66. Plaintiff Goodrum greatly values his privacy and Private Information and takes reasonable steps to maintain the confidentiality of his Private Information. Plaintiff Goodrum is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

67. Plaintiff Goodrum stores any and all documents containing Private Information in a secure location and destroys any documents he receives in the mail that contain any Private Information or that may contain any information that could otherwise be used to compromise his identity and credit card accounts.

68. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

69. As a result of the Data Breach, Plaintiff Goodrum's Private Information, including name and Social Security number, were published on the dark web.

70. As a result of the Data Breach, Plaintiff Goodrum has spent several hours researching the Data Breach, reviewing his bank accounts, monitoring his credit report, changing his passwords and other necessary mitigation efforts. This is valuable time that Plaintiff Goodrum would have spent on other activities, including but not limited to work and/or recreation.

71. As a consequence of and following the Data Breach, Plaintiff Goodrum has experienced a significant increase in spam calls, text messages, and emails, evidencing misuse of his Private Information.

72. The Data Breach has caused Plaintiff Goodrum to suffer fear, anxiety, and stress, which has been compounded by Defendant's delay in noticing him of the fact that his Social Security number was acquired by criminals as a result of the Data Breach.

73. Plaintiff Goodrum anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff Goodrum will continue to be at present and continued increased risk of identity theft and fraud for years to come.

74. Plaintiff Goodrum has a continuing interest in ensuring that his Private Information, which upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

75. As a direct and traceable result of the Data Breach, Plaintiff Goodrum suffered actual injury and damages after his Private Information was compromised and stolen in the Data

Breach, including, but not limited to: (a) lost time and money related to monitoring his accounts and credit reports for fraudulent activity; (b) loss of privacy due to his Private Information being accessed and stolen by cybercriminals; (c) loss of the benefit of the bargain because Defendant did not adequately protect his Private Information; (d) emotional distress because identity thieves now possess his first and last name paired with his Social Security number and other sensitive information; (e) imminent and impending injury arising from the increased risk of fraud and identity theft now that his Private Information has been stolen and likely published on the dark web; (f) diminution in the value of his Private Information, a form of intangible property that Defendant obtained from Plaintiff Goodrum and (g) other economic and non-economic harm.

***Plaintiff Marty Wooley's Experience***

76. Plaintiff Wooley is a current patient of Defendant's Client, Urology Associates of Mobile, P.A.

77. As a condition of obtaining medical services, Plaintiff Wooley was required to provide Defendant and its Client with her Private Information—including name, Social Security number, date of birth, medical and contact information.

78. Defendant was in possession of Plaintiff Wooley's Private Information before, during, and after the Data Breach.

79. Plaintiff Wooley reasonably understood and expected that Defendant would safeguard her Private Information and timely and adequately notify her in the event of a data breach. Plaintiff Wooley would not have allowed Defendant, or anyone in Defendant's position, to maintain her Private Information if she believed that Defendant would fail to implement reasonable and industry standard practices to safeguard that information from unauthorized access.

80. Plaintiff Wooley greatly values her privacy and Private Information and takes reasonable steps to maintain the confidentiality of her Private Information. Plaintiff Wooley is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

81. Plaintiff Wooley stores any and all documents containing Private Information in a secure location and destroys any documents she receives in the mail that contain any Private Information or that may contain any information that could otherwise be used to compromise her identity and credit card accounts.

82. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

83. As a result of the Data Breach, Plaintiff Wooley's Private Information, including name and Social Security number, were published on the dark web.

84. As a result of the Data Breach, Plaintiff Wooley has spent several hours researching the Data Breach, reviewing her bank accounts, monitoring her credit report, changing her passwords and other necessary mitigation efforts. This is valuable time that Plaintiff Wooley would have spent on other activities, including but not limited to work and/or recreation.

85. As a consequence of and following the Data Breach, Plaintiff Wooley has experienced a significant increase in spam calls, text messages, and emails, evidencing misuse of her Private Information.

86. The Data Breach has caused Plaintiff Wooley to suffer fear, anxiety, and stress, which has been compounded by Defendant's delay in noticing her of the fact that her Social Security number was acquired by criminals as a result of the Data Breach.

87. Plaintiff Wooley anticipates spending considerable time and money on an ongoing

basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff Wooley will continue to be at present and continued increased risk of identity theft and fraud for years to come.

88. Plaintiff Wooley has a continuing interest in ensuring that her Private Information, which upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

89. As a direct and traceable result of the Data Breach, Plaintiff Wooley suffered actual injury and damages after her Private Information was compromised and stolen in the Data Breach, including, but not limited to: (a) lost time and money related to monitoring her accounts and credit reports for fraudulent activity; (b) loss of privacy due to her Private Information being accessed and stolen by cybercriminals; (c) loss of the benefit of the bargain because Defendant did not adequately protect her Private Information; (d) emotional distress because identity thieves now possess her first and last name paired with her Social Security number and other sensitive information; (e) imminent and impending injury arising from the increased risk of fraud and identity theft now that her Private Information has been stolen and likely published on the dark web; (f) diminution in the value of her Private Information, a form of intangible property that Defendant obtained from Plaintiff Wooley and (g) other economic and non-economic harm.

***Plaintiff Todd Clay's Experience***

90. Plaintiff Clay is a current patient of Defendant's Client, Cabarrus Eye Center, P.A.

91. To obtain medical services, Plaintiff Clay was required to provide his Private Information to Defendant, including name, Social Security number, date of birth, address, phone number, and other sensitive information.

92. Upon information and belief, at the time of the Data Breach, Defendant retained Plaintiff Clay's Private Information.

93. Plaintiff Clay is very careful about sharing his sensitive Private Information. Plaintiff Clay stores any documents containing his Private Information in a safe and secure location. Plaintiff Clay has never knowingly transmitted unencrypted sensitive Private Information over the Internet or any other unsecured source.

94. As a result of the Data Breach, Plaintiff Clay made reasonable efforts to mitigate the impact of the Data Breach, including checking his bills and accounts to make sure they were correct. Plaintiff Clay has spent time dealing with the Data Breach, valuable time he otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

95. As a result of the Data Breach, Plaintiff Clay fears for his personal financial security and uncertainty over what medical information was revealed in the Data Breach. He is experiencing anxiety and fear because of the Data Breach and the invasion of his privacy. 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.

96. Furthermore, Plaintiff Clay's fears are compounded by the fact that his Private Information has already been published on the dark web because of the Data Breach.

97. As a result of the Data Breach, Plaintiff Clay anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

98. As a result of the Data Breach, Plaintiff Clay is presently at risk and will continue to be at increased risk of identity theft and fraud for years to come.

99. Plaintiff Clay has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains Defendant's possession, is protected and safeguarded from future breaches.

***Plaintiff Tanya Walker's Experience***

100. Plaintiff Walker is a current patient of Defendant's Client, North Buncombe

Family Medicine, P.A.

101. To obtain medical services from Defendant, Plaintiff Walker was required to provide her Private Information to Defendant, including name, Social Security number, date of birth, address, phone number, and other sensitive information.

102. Upon information and belief, at the time of the Data Breach, Defendant retained Plaintiff Walkers' Private Information.

103. Plaintiff Walker is very careful about sharing her sensitive Private Information. Plaintiff Walker stores any documents containing her Private Information in a safe and secure location. Plaintiff Walker has never knowingly transmitted unencrypted sensitive Private Information over the Internet or any other unsecured source.

104. As a result of the Data Breach, Plaintiff Walker made reasonable efforts to mitigate the impact of the Data Breach, including checking her bills and accounts to make sure they were correct. Plaintiff Walker has spent time dealing with the Data Breach, valuable time she otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

105. As a result of the Data Breach, Plaintiff Walker fears for her personal financial security and uncertainty over what medical information was revealed in the Data Breach. She is experiencing anxiety and fear because of the Data Breach and the invasion of her privacy. 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.

106. Furthermore, Plaintiff Walker's fears are compounded by the fact that her Private Information has already been published on the dark web, because of the Data Breach.

107. As a result of the Data Breach, Plaintiff Walker anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

108. As a result of the Data Breach, Plaintiff Walker is presently at risk and will continue to be at increased risk of identity theft and fraud for years to come.

109. Plaintiff Walker has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches

## CLASS ALLEGATIONS

110. Plaintiffs bring this amended class action complaint, individually and on behalf of the following Nationwide Class:

> Nationwide Class: All individuals whose Private Information was accessed and/or acquired by an unauthorized party in the Data Breach (the "Class").

111. Specifically excluded from the Class are Defendant, its officers, directors, agents, trustees, parents, children, corporations, trusts, representatives, principals, servants, partners, joint venturers, or entities controlled by Defendant, and its heirs, successors, assigns, or other persons or entities related to or affiliated with Defendant and/or its officers and/or directors, the judge assigned to this action, and any member of the judge's immediate family.

112. Plaintiffs reserve the right to amend the Class definitions above if further investigation and/or discovery reveals that the Class should be expanded, narrowed, divided into subclasses, or otherwise modified in any way.

113. This action may be certified as a class action because it satisfies the numerosity, commonality, typicality, adequacy, and superiority requirements therein.

114. Numerosity: The Class is so numerous that joinder of all Class Members is impracticable. Upon information and belief, Plaintiffs estimate that the Class is comprised of 1,275,807 members, if not more. The Class is sufficiently numerous to warrant certification.

115. Typicality of Claims: Plaintiffs claims are typical of those of other Class Members because Plaintiffs, like the unnamed Class, had their Private Information compromised as a result of the Data Breach. Plaintiffs are members of the Class, and their claims are typical of the claims

of the members of the Class. The harm suffered by Plaintiffs are similar to that suffered by all other Class Members which was caused by the same misconduct by Defendant.

116. Adequacy of Representation: Plaintiffs will fairly and adequately represent and protect the interests of the Class. Plaintiffs have no interests antagonistic to, nor in conflict with, the Class. Plaintiffs have retained competent counsel who are experienced in consumer and commercial class action litigation and who will prosecute this action vigorously.

117. Superiority: A class action is superior to other available methods for the fair and efficient adjudication of this controversy. Because the monetary damages suffered by individual Class Members are relatively small, the expense and burden of individual litigation make it impossible for individual Class Members to seek redress for the wrongful conduct asserted herein. If Class treatment of these claims is not available, Defendant will likely continue its wrongful conduct, will unjustly retain improperly obtained revenues, or will otherwise escape liability for its wrongdoing as asserted herein.

118. Predominant Common Questions: The claims of all Class Members present common questions of law or fact, which predominate over any questions affecting only individual Class Members, including:

a. Whether 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;

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

c. Whether Defendant's storage of Plaintiffs and Class Member's Private Information was done in a negligent manner;

d. Whether Defendant had a duty to protect and safeguard Plaintiffs and Class Members' Private Information;

e. Whether Defendant's conduct was negligent;

f. Whether Defendant's conduct violated Plaintiffs and Class Members' privacy;

g. Whether Defendant took sufficient steps to individuals' Private Information;

h. Whether Defendant was unjustly enriched; and

i. The nature of relief, including damages and equitable relief, to which Plaintiffs and Class Members are entitled.

119. Information concerning Defendant's policies is available from Defendant's records.

120. Plaintiffs know of no difficulty which will be encountered in the management of this litigation which would preclude its maintenance as a class action.

121. The prosecution of separate actions by individual members of the Class would run the risk of inconsistent or varying adjudications and establish incompatible standards of conduct for Defendant. Prosecution as a class action will eliminate the possibility of repetitious and inefficient litigation.

122. Given that Defendant has not indicated any changes to its conduct or security measures, monetary damages are insufficient and there is no complete and adequate remedy at law.

## COUNT I
## NEGLIGENCE
## (On behalf of Plaintiffs and the Nationwide Class)

123. Plaintiffs restate and reallege all of the allegations stated above as if fully set forth herein.

124. Defendant knowingly collected, possessed, and maintained Plaintiffs and Class Members' Private Information, and therefore had a duty to exercise reasonable care in safeguarding, securing, and protecting such Information from being disclosed, compromised, lost, stolen, and misused by unauthorized parties.

125. Defendant's duty also included a responsibility to implement processes by which it could detect and analyze a breach of its security systems quickly and to give prompt notice to those affected in the case of a cyberattack.

126. Defendant knew or should have known of the risks inherent in collecting the Private Information of Plaintiffs and Class Members and the importance of adequate security. Defendant was on notice because, on information and belief, it knew or should have known that it would be an attractive target for cyberattacks.

127. Defendant owed a duty of care to Plaintiffs and Class Members whose Private Information was entrusted to it. Defendant's duties included, but were not limited to, the following:

a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting Private Information in its possession;

b. To protect the Private Information in its possession it using reasonable and adequate security procedures and systems compliant with industry standards;

c. To have procedures in place to prevent the loss or unauthorized dissemination of Private Information in its possession;

d. To employ reasonable security measures and otherwise protect the Private Information of Plaintiffs and Class Members pursuant to HIPAA and the FTCA;

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

f. To promptly notify Plaintiffs and Class Members of the Data Breach, and to precisely disclose the type(s) of information compromised.

128. Defendant's duty to employ reasonable data security measures arose, in part, under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which 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.

129. Defendant's duty also arose because Defendant was bound by industry standards to protect the confidential Private Information entrusted to it.

130. Plaintiffs and Class Members were foreseeable victims of any inadequate security practices on the part of Defendant, and Defendant owed them a duty of care to not subject them to an unreasonable risk of harm.

131. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiffs and Class Members by failing to exercise reasonable care in protecting and safeguarding Plaintiffs and Class Members' Private Information within Defendant's possession.

132. Defendant, by its actions and/or omissions, breached its duty of care by failing to provide, or acting with reckless disregard for, fair, reasonable, or adequate computer systems and data security practices to safeguard the Private Information of Plaintiffs and Class Members.

133. Defendant, by its actions and/or omissions, breached its duty of care by failing to promptly identify the Data Breach and then failing to provide prompt notice of the Data Breach to the persons whose Private Information was compromised.

134. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Plaintiffs and Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

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

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

c. Failing to periodically ensure that its email system maintained reasonable data security safeguards;

d. Allowing unauthorized access to Class Members' Private Information;

e. Failing to comply with the FTCA and HIPAA;

f. Failing to detect in a timely manner that Class Members' Private Information 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.

135. Defendant acted with reckless disregard for the rights of Plaintiffs and Class Members by failing to provide prompt and adequate individual notice of the Data Breach such that Plaintiffs and Class Members could take measures to protect themselves from damages caused by the fraudulent use of the Private Information compromised in the Data Breach.

136. Defendant had a special relationship with Plaintiffs and Class Members. Plaintiffs and Class Members' willingness to entrust Defendant with their Private Information was predicated on the understanding that Defendant would take adequate security precautions. Moreover, only Defendant had the ability to protect its systems (and the Private Information that it stored on them) from attack.

137. Defendant's breach of duties owed to Plaintiffs and Class Members caused Plaintiffs and Class Members' Private Information to be compromised and exfiltrated, as alleged herein.

138. As a result of Defendant's ongoing failure to notify Plaintiffs and Class Members regarding the Data Breach, Plaintiffs and Class Members have been unable to take the necessary precautions to prevent future fraud and mitigate damages.

139. Defendant's breaches of duty also caused a substantial, imminent risk to Plaintiffs and Class Members of identity theft, loss of control over their Private Information, and loss of time and money to monitor their accounts for fraud.

140. As a result of Defendant's negligence in breach of its duties owed to Plaintiffs and Class Members, Plaintiffs and Class Members are in danger of imminent harm in that their Private Information, which is still in the possession of third parties, will be used for fraudulent purposes.

141. Defendant also had independent duties under state laws that required it to reasonably safeguard Plaintiffs and Class Members' Private Information and promptly notify them about the Data Breach.

142. As a direct and proximate result of Defendant's negligent conduct, Plaintiffs and Class Members have suffered damages as alleged herein and are at imminent risk of further harm.

143. The injury and harm that Plaintiffs and Class Members suffered was reasonably foreseeable.

144. Plaintiffs and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

145. In addition to monetary relief, Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to, *inter alia*, strengthen its data security systems and

monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members.

**COUNT II**
**NEGLIGENCE *PER SE***
**(On behalf of Plaintiffs and the Nationwide Class**

146. Plaintiffs restate and reallege the allegations in the preceding paragraphs as if fully set forth herein.

147. Pursuant to Section 5 of the FTCA, Defendant had a duty to provide fair and adequate computer systems and data security to safeguard the Private Information of Plaintiffs and Class Members.

148. Pursuant to HIPAA, 42 U.S.C. § 1302(d), *et seq*., Defendant had a duty to implement reasonable safeguards to protect Plaintiffs and Class Members' Private Information.

149. Specifically, pursuant to HIPAA, Defendant had a duty to render the electronic PHI it maintained unusable, unreadable, or indecipherable to unauthorized individuals by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without the use of a confidential process or key." *See* definition of "encryption" at 45 C.F.R. § 164.304.

150. Defendant breached its duties to Plaintiffs and Class Members under the FTCA and HIPAA by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs and Class Members' Private Information.

151. Specifically, Defendant breached its duties by failing to employ industry-standard cybersecurity measures in order to comply with the FTCA, including but not limited to proper segregation, access controls, password protection, encryption, intrusion detection, secure destruction of unnecessary data, and penetration testing.

152. The FTCA prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice of failing to use reasonable measures to protect PII and PHI (such as the Private Information compromised in the Data Breach). The FTC rulings and publications described above, together with the industry-standard cybersecurity measures set forth herein, form part of the basis of Defendant's duty in this regard.

153. Defendant also violated the FTCA and HIPAA by failing to use reasonable measures to protect the Private Information of Plaintiffs and the Class and by not complying with applicable industry standards, as described herein.

154. It was reasonably foreseeable, particularly given the growing number of data breaches of Private Information, that the failure to reasonably protect and secure Plaintiffs and Class Members' Private Information in compliance with applicable laws would result in an unauthorized third-party gaining access to Defendant's networks, databases, and computers that stored Plaintiff's and Class Members' unencrypted Private Information.

155. Plaintiffs and Class Members are within the class of persons that the FTCA and HIPAA are intended to protect and Defendant's failure to comply with both constitutes negligence *per se*.

156. Plaintiffs and Class Members' Private Information constitutes personal property that was stolen due to Defendant's negligence, resulting in harm, injury, and damages to Plaintiffs and Class Members.

157. As a direct and proximate result of Defendant's negligence *per se*, Plaintiffs and the Class have suffered, and continue to suffer, injuries and damages arising from the unauthorized access of their Private Information, including but not limited to damages from the lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives.

158. As a direct and proximate result of Defendant's negligent conduct, Plaintiffs and Class Members have suffered injury and are entitled to compensatory and consequential damages in an amount to be proven at trial.

159. In addition to monetary relief, Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members.

## COUNT III
## BREACH OF THIRD-PARTY BENEFICIARY CONTRACT
## (ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS)

160. Plaintiffs restate and reallege the allegations in the preceding paragraphs as if fully set forth herein.

161. Defendant entered into contracts, written or implied, with its Clients to perform services that include, but are not limited to, providing medical coding and risk adjustment services. Upon information and belief, these contracts are virtually identical between and among Defendant and its Clients around the country whose customers and patients, including Plaintiffs and Class Members, were affected by the Data Breach.

162. In exchange, Defendant agreed, in part, to implement adequate security measures to safeguard the Private Information of Plaintiffs and the Class.

163. These contracts were made expressly for the benefit of Plaintiffs and the Class, as Plaintiffs and Class Members were the intended third-party beneficiaries of the contracts entered into between Defendant and its Clients. Defendant knew that if it were to breach these contracts with its Clients, its Clients' policyholders and patients—Plaintiffs and Class Members—would be harmed.

164. Defendant breached the contracts it entered into with its Clients by, among other things, failing to (i) use reasonable data security measures, (ii) implement adequate protocols and employee training sufficient to protect Plaintiffs Private Information from unauthorized disclosure to third parties, and (iii) promptly and adequately detecting the Data Breach and notifying Plaintiffs and Class Members thereof.

165. Plaintiffs and the Class were harmed by Defendant's breach of its contracts with its clients, as such breach is alleged herein, and are entitled to the losses and damages they have sustained as a direct and proximate result thereof.

166. Plaintiffs and Class Members are also entitled to their costs and attorney's fees incurred in this action.

## COUNT IV
## UNJUST ENRICHMENT
## (On behalf of Plaintiffs and the Nationwide Class)

167. Plaintiffs restate and reallege the allegations in the preceding paragraphs as if fully set forth herein.

168. This Count is pleaded in the alternative to Count III above.

169. Plaintiffs and Class Members conferred a benefit on Defendant by permitting their healthcare providers and healthcare plans to turn over their Private Information to Defendant. Moreover, upon information and belief, Plaintiffs allege that payments made by Defendant's Clients to Defendant included payment for cybersecurity protection to protect Plaintiffs and Class Members' Private Information, and that those cybersecurity costs were passed on to Plaintiffs and Class Members in the form of elevated prices charged by Defendant Clients for their services. Plaintiffs and Class Members did not receive such protection.

170. Upon information and belief, Defendant funds its data security measures entirely from its general revenue, including from payments made to it by its Clients on behalf of Plaintiffs and Class Members.

171. As such, a portion of the payments made by Plaintiffs and Class Members is to be used to provide a reasonable and adequate level of data security that is in compliance with applicable state and federal regulations and industry standards, and the amount of the portion of each payment made that is allocated to data security is known to Defendant.

172. Defendant has retained the benefits of its unlawful conduct, including the amounts of payment received indirectly from Plaintiffs and Class Members that should have been used for adequate cybersecurity practices that it failed to provide.

173. Defendant knew that Plaintiffs and Class Members conferred a benefit upon it, which Defendant accepted. Defendant profited from these transactions and used the Private Information of Plaintiffs and Class Members for business purposes, while failing to use the payments it received for adequate data security measures that would have secured Plaintiffs and Class Members' Private Information and prevented the Data Breach.

174. If Plaintiffs and Class Members had known that Defendant had not adequately secured their Private Information, they would not have agreed to provide such Private Information to Defendant.

175. Due to Defendant's conduct alleged herein, it would be unjust and inequitable under the circumstances for Defendant's to be permitted to retain the benefit of its wrongful conduct.

176. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered, and/or are at a continued, imminent risk of suffering, injury that includes but is not limited to the following: (i) actual identity theft; (ii) the loss of the opportunity to control

how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (v) 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; (vi) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Private Information in its continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

177. Plaintiffs and Class Members are entitled to full refunds, restitution, and/or damages from Defendant and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Defendant from its wrongful conduct. This can be accomplished by establishing a constructive trust from which the Plaintiffs and Class Members may seek restitution or compensation.

178. Plaintiffs and Class Members may not have an adequate remedy at law against Defendant, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

## COUNT V
## DECLARATORY JUDGMENT
## (On behalf of Plaintiffs and the Nationwide Class)

179. Plaintiffs restate and reallege the allegations in the preceding paragraphs as if fully set forth herein.

180. Under the Declaratory Judgment Act, 28 U.S.C. § 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and to grant further necessary relief. Furthermore, the Court has broad authority to restrain acts that are tortious and violate the terms of the federal laws and regulations described in this Complaint.

181. Defendant owes a duty of care to Plaintiffs and Class Members, which required it to adequately secure Plaintiffs and Class Members' Private Information.

182. Defendant still possesses Private Information regarding Plaintiffs and Class Members.

183. Plaintiffs alleges that Defendant's data security measures remain inadequate. Furthermore, Plaintiffs continue to suffer injury as a result of the compromise of their Private Information and the risk remains that further compromises of their Private Information will occur in the future.

184. Under its authority pursuant to the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendant owes a legal duty to secure its Clients' policyholders' and patients' Private Information and to timely notify them of a data breach under the common law, HIPAA, and the FTCA;

b. Defendant's existing security measures do not comply with its explicit or implicit contractual obligations and duties of care to provide reasonable security procedures and practices that are appropriate to protect patient Private Information; and

c. Defendant continues to breach this legal duty by failing to employ reasonable measures to secure its Clients' customers' and patients' Private Information.

185. This Court should also issue corresponding prospective injunctive relief requiring Defendant to employ adequate security protocols consistent with legal and industry standards to protect patient and customer Private Information in its possession, including the following:

a. Order Defendant to provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members.

b. Order that, to comply with Defendant's explicit or implicit contractual obligations and duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to:

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

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

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

iv. segmenting its user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Defendant's systems;

v. conducting regular database scanning and security checks;

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

vii. meaningfully educating its Clients and their patients and customers about the threats they face with regard to the security of their Private Information, as well as the steps they should take to protect themselves.

186. If an injunction is not issued, Plaintiffs will suffer irreparable injury and will lack an adequate legal remedy to prevent another data breach at Defendant. The risk of another such breach is real, immediate, and substantial. If another breach at Defendant occurs, Plaintiffs will not have an adequate remedy at law because many of the resulting injuries are not readily quantifiable.

187. The hardship to Plaintiffs if an injunction is not issued exceeds the hardship to Defendant if an injunction is issued. Plaintiffs will likely be subjected to substantial, continued identity theft and other related damages if an injunction is not issued. On the other hand, the cost of Defendant's compliance with an injunction requiring reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

188. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing a subsequent data breach at Defendant, thus preventing future injury to Plaintiffs, Class Members, and others whose Private Information would be further compromised.

## PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and the Class described above, seek the following relief:

a. An order certifying this action as a Class action under Fed. R. Civ. P. 23, defining the Class as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiffs are proper representatives of the Nationwide Class requested herein;

b. Judgment in favor of Plaintiffs and Class Members awarding them appropriate monetary relief, including actual damages, statutory damages, equitable relief, restitution, disgorgement, and statutory costs;

c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class as requested herein;

d. An order instructing Defendant to purchase or provide funds for lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members;

e. An order requiring Defendant to pay the costs involved in notifying Class Members about the judgment and administering the claims process;

f. A judgment in favor of Plaintiffs and Class Members awarding them prejudgment and post-judgment interest, reasonable attorneys' fees, costs, and expenses as allowable by law; and

g. An award of such other and further relief as this Court may deem just and proper.

**DEMAND FOR JURY TRIAL**

Plaintiffs demand a trial by jury of all claims in this Class Action Complaint so triable.

Dated: August 30, 2025.

Respectfully,

/s/ *Gary M. Klinger*

Gary M. Klinger
**MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC**
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Tele: 866.252.0878
gklinger@milberg.com

Jeff Ostrow
**KOPELOWITZ OSTROW P.A.**
One West Law Olas Blvd., Suite 500
Fort Lauderdale, Florida 33301
Tele: (954) 612-4100
ostrow@kolawyers.com

*Attorneys for Plaintiffs and the Proposed Class*

**CERTIFICATE OF SERVICE**

I hereby certify that on this 30th day of August 2025, I caused a true and correct copy of the foregoing to be filed with the Clerk of the Court via the Court's CM/ECF system which will deliver electronic service to all counsel of record.

/s/ *Gary M. Klinger*
Gary M. Klinger