

**UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY**

JAMIE KEEFER, on behalf of himself and all
others similarly situated,

Plaintiff,

v.

**AMERICAN NEIGHBORHOOD
MORTGAGE ACCEPTANCE COMPANY,
LLC D/B/A ANNIEMAC HOME
MORTGAGE**,

Defendant.

No.

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

Jamie Keefer (“Plaintiff”), through his attorneys, individually and on behalf of all others similarly situated, brings this Class Action Complaint against Defendant American Neighborhood Mortgage Acceptance Company, LLC d/b/a AnnieMac Home Mortgage (“AnnieMac” or “Defendant”), and its present, former, or future direct and indirect parent companies, subsidiaries, affiliates, agents, and/or other related entities. Plaintiff alleges the following on information and belief—except as to his own actions, counsel’s investigations, and facts of public record.

NATURE OF ACTION

1. This class action arises from Defendant’s failure to protect highly sensitive data.
2. Defendant is a home mortgage company based in Mount Laurel, New Jersey.¹
3. As such, Defendant stores a litany of highly sensitive personal identifiable information (“PII”) about its current and former customers. But Defendant lost control over that

¹ *Home Page*, ANNIE MAC, <https://www.annie-mac.com/> (last visited Nov. 22, 2024).

data when cybercriminals infiltrated its insufficiently protected computer systems in a data breach (the “Data Breach”).

4. It is unknown for precisely how long the cybercriminals had access to Defendant’s network before the breach was discovered. In other words, Defendant had no effective means to prevent, detect, stop, or mitigate breaches of its systems—thereby allowing cybercriminals unrestricted access to its current and former customers’ PII.

5. On information and belief, cybercriminals were able to breach Defendant’s systems because Defendant failed to adequately train its employees on cybersecurity and failed to maintain reasonable security safeguards or protocols to protect the Class’s PII. In short, Defendant’s failures placed the Class’s PII in a vulnerable position—rendering them easy targets for cybercriminals.

6. Plaintiff is a Data Breach victim, having received a breach notice. He brings this class action on behalf of himself, and all others harmed by Defendant’s misconduct.

7. The exposure of one’s PII to cybercriminals is a bell that cannot be unring. Before this data breach, its current and former customers’ private information was exactly that—private. Not anymore. Now, their private information is forever exposed and unsecure.

PARTIES

8. Plaintiff, Jamie Keefer, is a natural person and citizen of Pennsylvania where he intends to remain.

9. Defendant, American Neighborhood Mortgage Acceptance Company, LLC d/b/a AnnieMac Home Mortgage, is a limited liability company formed under the laws of Delaware and with its principal place of business at 700 East Gate Drive, Suite 400, Mount Laurel, New Jersey 08054.

JURISDICTION AND VENUE

10. This Court has subject matter 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. Plaintiff and Defendant are citizens of different states.² And there are over 100 putative Class Members.

11. This Court has personal jurisdiction over Defendant because it is headquartered in New Jersey, regularly conducts business in New Jersey, and has sufficient minimum contacts in New Jersey.

12. Venue is proper in this Court because Defendant's principal office is in this District, and because a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in this District.

BACKGROUND

Defendant Collected and Stored the PII of Plaintiff and the Class

13. Defendant is a home mortgage company based in Mount Laurel, New Jersey.³

14. As part of its business, Defendant receives and maintains the PII of thousands of its current and former customers.

15. In collecting and maintaining the PII, Defendant agreed it would safeguard the data in accordance with its internal policies, state law, and federal law. After all, Plaintiff and Class Members themselves took reasonable steps to secure their PII.

² Under the Class Action Fairness Act, "an unincorporated association shall be deemed to be a citizen of the State where it has its principal place of business and the State under whose laws it is organized." 28 U.S.C. § 1332(d)(10). Thus, as an LLC, Defendant American Neighborhood Mortgage Acceptance Company, LLC is a citizen of Delaware (state of formation) and New Jersey (principal place of business).

³ *Home Page*, ANNIE MAC, <https://www.annie-mac.com/> (last visited Nov. 22, 2024).

16. Under state and federal law, businesses like Defendant have duties to protect its current and former customers' PII and to notify them about breaches.

17. Defendant recognizes these duties, declaring in its "Privacy Policy" that:

- a. "We restrict access to nonpublic personal information about you to those employees who need to know that information to provide products or services to you."⁴
- b. "We maintain physical, electronic, and procedural safeguards that comply with federal regulations to guard your nonpublic personal information."⁵
- c. "We use industry-standard methods to protect your personally identifiable information from unauthorized access."⁶
- d. "Among other techniques, we usually store such information on a computer behind our 'firewall' in a secure location, and we often restrict the number of employees internally who can access such data."⁷

Defendant's Data Breach

18. On August 21, 2024, Defendant was hacked in the Data Breach.⁸

19. Worryingly, Defendant already admitted that "between August 21, 2024 and August 23, 2024, an unknown actor gained access to systems on AnnieMac's network and viewed and/or copied certain files from these systems."⁹

⁴ *Privacy Policy*, ANNIE MAC, <https://www.annie-mac.com/page/privacy> (last visited Nov. 22, 2024).

⁵ *Id.*

⁶ *Id.*

⁷ *Id.*

⁸ Data Breach Notifications, MAINE ATTY GEN, <https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/4e82f3bb-55b2-4dd5-bd97-86893bddd75d.html> (last visited Nov. 22, 2024).

⁹ *Id.*

20. Because of Defendant’s Data Breach, at least the following types of PII were compromised: names and Social Security numbers.¹⁰

21. In total, Defendant injured at least 171,074 persons—via the exposure of their PII—in the Data Breach.¹¹ Upon information and belief, these 171,074 persons include its current and former customers.

22. And yet, Defendant waited over until November 14, 2024, before it began notifying the Class. Thus, Defendant kept the Class in the dark—thereby depriving the Class of the opportunity to try and mitigate their injuries in a timely manner.

23. And when Defendant did notify Plaintiff and the Class of the Data Breach, Defendant acknowledged that the Data Breach created a present, continuing, and significant risk of suffering identity theft, warning Plaintiff and the Class they needed to invest their time, time they would never get back, in trying to compensate for Defendant’s unlawful or negligent conduct:

- a. “We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors over the next 12 to 24 months.”¹²

24. Defendant failed its duties when its inadequate security practices caused the Data Breach. In other words, Defendant’s negligence is evidenced by its failure to prevent the Data Breach and stop cybercriminals from accessing the PII. And thus, Defendant caused widespread injury and monetary damages.

¹⁰ *Id.*

¹¹ *Id.*

¹² *Id.*

25. Since the breach, Defendant claims to have “implemented additional security measures to further protect against similar incidents occurring in the future.”¹³

26. But such simple declarations are insufficient to ensure that Plaintiff’s and Class Members’ PII will be protected from additional exposure in a subsequent data breach.

27. Defendant has done little to remedy its Data Breach. True, Defendant has offered some victims credit monitoring and identity related services. But upon information and belief, such services are wholly insufficient to compensate Plaintiff and Class Members for the injuries that Defendant inflicted upon them.

28. Because of Defendant’s Data Breach, the sensitive PII of Plaintiff and Class Members was placed into the hands of cybercriminals—inflicting numerous injuries and significant damages upon Plaintiff and Class Members.

29. Upon information and belief, the cybercriminals in question are particularly sophisticated. After all, the cybercriminals: (1) defeated the relevant data security systems, (2) gained actual access to sensitive data, and (3) successfully acquired data.

30. And as the Harvard Business Review notes, such “[c]ybercriminals frequently use the Dark Web—a hub of criminal and illicit activity—to sell data from companies that they have gained unauthorized access to through credential stuffing attacks, phishing attacks, [or] hacking.”¹⁴

31. Thus, on information and belief, Plaintiff’s and the Class’s stolen PII has already been published—or will be published imminently—by cybercriminals on the Dark Web.

¹³ *Id.*

¹⁴ Brenda R. Sharton, *Your Company’s Data Is for Sale on the Dark Web. Should You Buy It Back?*, HARVARD BUS. REV. (Jan. 4, 2023) <https://hbr.org/2023/01/your-companys-data-is-for-sale-on-the-dark-web-should-you-buy-it-back>.

Plaintiff's Experiences and Injuries

32. Plaintiff Jamie Keefer is a former customer of Defendant—having inquired about receiving a home loan.

33. Thus, Defendant obtained and maintained Plaintiff's PII.

34. As a result, Plaintiff was injured by Defendant's Data Breach.

35. Plaintiff provided his PII to Defendant and trusted the company would use reasonable measures to protect it according to Defendant's internal policies, as well as state and federal law. Defendant obtained and continues to maintain Plaintiff's PII and has a continuing legal duty and obligation to protect that PII from unauthorized access and disclosure.

36. Plaintiff reasonably understood that a portion of the funds paid to Defendant would be used to pay for adequate cybersecurity and protection of PII.

37. Plaintiff received a Notice of Data Breach.

38. Thus, on information and belief, Plaintiff's PII has already been published—or will be published imminently—by cybercriminals on the Dark Web.

39. Through its Data Breach, Defendant compromised Plaintiff's name and Social Security number.

40. Plaintiff has spent—and will continue to spend—significant time and effort monitoring his accounts to protect himself from identity theft. After all, Defendant directed Plaintiff to take those steps in its breach notice.

41. Plaintiff fears for his personal financial security and worries about what information was exposed in the Data Breach.

42. Because of Defendant's Data Breach, Plaintiff has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond

allegations of mere worry or inconvenience. Rather, Plaintiff's injuries are precisely the type of injuries that the law contemplates and addresses.

43. Plaintiff suffered actual injury from the exposure and theft of his PII—which violates his rights to privacy.

44. Plaintiff suffered actual injury in the form of damages to and diminution in the value of his PII. After all, PII is a form of intangible property—property that Defendant was required to adequately protect.

45. Plaintiff suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because Defendant's Data Breach placed Plaintiff's PII right in the hands of criminals.

46. Because of the Data Breach, Plaintiff anticipates spending considerable amounts of time and money to try and mitigate his injuries.

47. Today, Plaintiff has a continuing interest in ensuring that his PII—which, upon information and belief, remains backed up in Defendant's possession—is protected and safeguarded from additional breaches.

Plaintiff and the Proposed Class Face Significant Risk of Continued Identity Theft

48. Because of Defendant's failure to prevent the Data Breach, Plaintiff and Class Members suffered—and will continue to suffer—damages. These damages include, *inter alia*, monetary losses, lost time, anxiety, and emotional distress. Also, they suffered or are at an increased risk of suffering:

- a. loss of the opportunity to control how their PII is used;
- b. diminution in value of their PII;
- c. compromise and continuing publication of their PII;

- d. out-of-pocket costs from trying to prevent, detect, and recovery from identity theft and fraud;
- e. lost opportunity costs and wages from spending time trying to mitigate the fallout of the Data Breach by, *inter alia*, preventing, detecting, contesting, and recovering from identify theft and fraud;
- f. delay in receipt of tax refund monies;
- g. unauthorized use of their stolen PII; and
- h. continued risk to their PII—which remains in Defendant’s possession—and is thus as risk for futures breaches so long as Defendant fails to take appropriate measures to protect the PII.

49. 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.

50. The value of Plaintiff and Class’s PII on the black market is considerable. Stolen PII trades on the black market for years. And criminals frequently post and sell stolen information openly and directly on the “Dark Web”—further exposing the information.

51. It can take victims years to discover such identity theft and fraud. This gives criminals plenty of time to sell the PII far and wide.

52. One way that criminals profit from stolen PII is by creating comprehensive dossiers on individuals called “Fullz” packages. These dossiers are both shockingly accurate and comprehensive. Criminals create them by cross-referencing and combining two sources of data—first the stolen PII, and second, unregulated data found elsewhere on the internet (like phone numbers, emails, addresses, etc.).

53. The development of “Fullz” packages means that the PII exposed in the Data Breach can easily be linked to data of Plaintiff and the Class that is available on the internet.

54. 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 Class Members, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff and other Class Members’ stolen PII is being misused, and that such misuse is fairly traceable to the Data Breach.

55. Defendant disclosed the PII of Plaintiff and Class Members for criminals to use in the conduct of criminal activity. Specifically, Defendant opened up, disclosed, and exposed the PII of Plaintiff and Class Members 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.

56. Defendant’s failure to promptly and properly notify Plaintiff and Class Members of the Data Breach exacerbated Plaintiff and Class Members’ 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.

Defendant Knew—Or Should Have Known—of the Risk of a Data Breach

57. Defendant’s data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in recent years.

58. In 2021, a record 1,862 data breaches occurred, exposing approximately

293,927,708 sensitive records—a 68% increase from 2020.¹⁵

59. Indeed, cyberattacks have become so notorious that the Federal Bureau of Investigation (“FBI”) and U.S. Secret Service issue warnings to potential targets, so they are aware of, and prepared for, a potential attack. As one report explained, “[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals . . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly.”¹⁶

60. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant’s industry, including Defendant.

Defendant Failed to Follow FTC Guidelines

61. According to the Federal Trade Commission (“FTC”), the need for data security should be factored into all business decision-making. Thus, the FTC issued numerous guidelines identifying best data security practices that businesses—like Defendant—should use to protect against unlawful data exposure.

62. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*. There, the FTC set guidelines for what data security principles and practices businesses must use.¹⁷ The FTC declared that, *inter alia*, businesses must:

- a. protect the personal customer information that they keep;
- b. properly dispose of personal information that is no longer needed;

¹⁵ See *2021 Data Breach Annual Report*, IDENTITY THEFT RESOURCE CENTER (Jan. 2022) <https://notified.idtheftcenter.org/s/>.

¹⁶ Ben Kochman, *FBI, Secret Service Warn of Targeted Ransomware*, LAW360 (Nov. 18, 2019), <https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware>.

¹⁷ *Protecting Personal Information: A Guide for Business*, FED TRADE COMMISSION (Oct. 2016) https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

- c. encrypt information stored on computer networks;
- d. understand their network's vulnerabilities; and
- e. implement policies to correct security problems.

63. The guidelines also recommend that businesses watch for the transmission of large amounts of data out of the system—and then have a response plan ready for such a breach.

64. Furthermore, the FTC explains that companies must:

- a. not maintain information longer than is needed to authorize a transaction;
- b. limit access to sensitive data;
- c. require complex passwords to be used on networks;
- d. use industry-tested methods for security;
- e. monitor for suspicious activity on the network; and
- f. verify that third-party service providers use reasonable security measures.

65. The FTC brings enforcement actions against businesses for failing to protect customer data adequately and reasonably. Thus, the FTC treats the failure—to use reasonable and appropriate measures to protect against unauthorized access to confidential consumer data—as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act (“FTCA”), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

66. In short, Defendant's failure to use reasonable and appropriate measures to protect against unauthorized access to its current and former customers' data constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

Defendant Failed to Follow Industry Standards

67. Several best practices have been identified that—at a *minimum*—should be implemented by businesses like Defendant. These industry standards include: 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 industry standard best practices 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; and training staff regarding critical points.

69. Upon information and belief, Defendant failed to implement industry-standard cybersecurity measures, including failing to meet the minimum standards of both the NIST Cybersecurity Framework Version 2.0 (including without limitation PR.AA-01, PR.AA-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01, PR.DS-01, PR.DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, and RS.CO-04) and the Center for Internet Security’s Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

70. These frameworks are applicable and accepted industry standards. And by failing to comply with these accepted standards, Defendant opened the door to the criminals—thereby causing the Data Breach.

CLASS ACTION ALLEGATIONS

71. Plaintiff brings this class action under Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3), individually and on behalf of all members of the following class:

All individuals residing in the United States whose PII was compromised in the Data Breach discovered by AnnieMac in August 2024, including all those individuals who received notice of the breach.

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

73. Plaintiff reserves the right to amend the class definition.

74. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of his claims on class-wide bases using the same evidence as would be used to prove those elements in individual actions asserting the same claims.

75. Ascertainability. All members of the proposed Class are readily ascertainable from information in Defendant's custody and control. After all, Defendant already identified individuals affected and sent them data breach notices.

76. Numerosity. The Class Members are so numerous that joinder of all Class Members is impracticable. Upon information and belief, the proposed Class includes at least 171,074 members.

77. Typicality. Plaintiff's claims are typical of Class Members' claims as each arises from the same Data Breach, the same alleged violations by Defendant, and the same unreasonable manner of notifying individuals about the Data Breach.

78. Adequacy. Plaintiff will fairly and adequately protect the proposed Class's common interests. His interests do not conflict with Class Members' interests. And Plaintiff has retained counsel—including lead counsel—that is experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf.

79. Commonality and Predominance. Plaintiff's and the Class's claims raise predominantly common fact and legal questions—which predominate over any questions affecting individual Class Members—for which a class wide proceeding can answer for all Class Members.

In fact, a class wide proceeding is necessary to answer the following questions:

- a. if Defendant had a duty to use reasonable care in safeguarding Plaintiff's and the Class's 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 was negligent in maintaining, protecting, and securing PII;
- d. if Defendant breached contract promises to safeguard Plaintiff and the Class's PII;
- e. if Defendant took reasonable measures to determine the extent of the Data Breach after discovering it;
- f. if Defendant's Breach Notice was reasonable;
- g. if the Data Breach caused Plaintiff and the Class injuries;
- h. what the proper damages measure is; and
- i. if Plaintiff and the Class are entitled to damages, treble damages, and or injunctive relief.

80. Superiority. A class action will provide substantial benefits and is superior to all other available means for the fair and efficient adjudication of this controversy. The damages or other financial detriment suffered by individual Class Members are relatively small compared to the burden and expense that individual litigation against Defendant would require. Thus, it would

be practically impossible for Class Members, on an individual basis, to obtain effective redress for their injuries. Not only would individualized litigation increase the delay and expense to all parties and the courts, but individualized litigation would also create the danger of inconsistent or contradictory judgments arising from the same set of facts. By contrast, the class action device provides the benefits of adjudication of these issues in a single proceeding, ensures economies of scale, provides comprehensive supervision by a single court, and presents no unusual management difficulties.

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

81. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

82. Plaintiff and the Class entrusted their PII to Defendant on the premise and with the understanding that Defendant would safeguard their PII, use their PII for business purposes only, and/or not disclose their PII to unauthorized third parties.

83. Defendant owed a duty of care to Plaintiff and Class Members because it was foreseeable that Defendant's failure—to use adequate data security in accordance with industry standards for data security—would compromise their PII in a data breach. And here, that foreseeable danger came to pass.

84. Defendant has full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and the Class could and would suffer if their PII was wrongfully disclosed.

85. 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 Defendant's inadequate security practices. After all, Defendant actively sought and obtained Plaintiff and Class Members' PII.

86. Defendant owed—to Plaintiff and Class Members—at least the following duties to:
- a. exercise reasonable care in handling and using the PII in its care and custody;
 - b. implement industry-standard security procedures sufficient to reasonably protect the information from a data breach, theft, and unauthorized;
 - c. promptly detect attempts at unauthorized access;
 - d. notify Plaintiff and Class Members within a reasonable timeframe of any breach to the security of their PII.

87. Thus, Defendant owed a duty to timely and accurately disclose to Plaintiff and Class Members the scope, nature, and occurrence of the Data Breach. After all, this duty is required and necessary for Plaintiff and Class Members to take appropriate measures to protect their PII, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

88. Defendant also had a duty to exercise appropriate clearinghouse practices to remove PII it was no longer required to retain under applicable regulations.

89. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the PII of Plaintiff and the Class involved an unreasonable risk of harm to Plaintiff and the Class, even if the harm occurred through the criminal acts of a third party.

90. Defendant's duty to use reasonable security measures arose because of the special relationship that existed between Defendant and Plaintiff and the Class. That special relationship arose because Plaintiff and the Class entrusted Defendant with their confidential PII, a necessary part of obtaining services from Defendant.

91. The risk that unauthorized persons would attempt to gain access to the PII and misuse it was foreseeable. Given that the Defendant holds vast amounts of PII, it was inevitable that unauthorized individuals would attempt to access Defendant's databases containing the PII — whether by malware or otherwise.

92. 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' and the importance of exercising reasonable care in handling it.

93. Defendant improperly and inadequately safeguarded the PII of Plaintiff and the Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

94. Defendant breached these duties as evidenced by the Data Breach.

95. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiff's and Class Members' PII by:

- a. disclosing and providing access to this information to third parties and
- b. failing to properly supervise both the way the PII was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

96. Defendant breached its duties by failing to exercise reasonable care in supervising its agents, contractors, vendors, and suppliers, and in handling and securing the personal information and PII of Plaintiff and Class Members which actually and proximately caused the Data Breach and Plaintiff and Class Members' injury.

97. Defendant further breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiff and Class Members, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiff and Class Members' injuries-in-fact.

98. Defendant has admitted that the PII of Plaintiff and the Class was wrongfully lost and disclosed to unauthorized third persons because of the Data Breach.

99. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiff and Class Members have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

100. And, on information and belief, Plaintiff's PII has already been published—or will be published imminently—by cybercriminals on the Dark Web.

101. Defendant's breach of its common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiff and Class Members actual, tangible, injury-in-fact and damages, including, without limitation, 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, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

SECOND CAUSE OF ACTION
Negligence per se
(On Behalf of Plaintiff and the Class)

102. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

103. Under the FTC Act, 15 U.S.C. § 45, Defendant had a duty to use fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' PII.

104. Section 5 of the FTC Act prohibits “unfair . . . practices in or affecting commerce,” including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect the PII entrusted to it. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant’s duty to protect Plaintiff and the Class Members’ sensitive PII.

105. Defendant breached its respective duties to Plaintiff and Class Members under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard PII.

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

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

108. But for Defendant’s wrongful and negligent breach of its duties owed, Plaintiff and Class Members would not have been injured.

109. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendant’s breach of their duties. Defendant knew or should have known

that Defendant was failing to meet its duties and that its breach would cause Plaintiff and members of the Class to suffer the foreseeable harms associated with the exposure of their PII.

110. Defendant's various violations and its failure to comply with applicable laws and regulations constitutes negligence *per se*.

111. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and Class Members have suffered and will continue to suffer numerous injuries (as detailed *supra*).

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

112. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

113. Plaintiff and Class Members either directly contracted with Defendant or Plaintiff and Class Members were the third-party beneficiaries of contracts with Defendant.

114. Plaintiff and Class Members were required to provide their PII to Defendant as a condition of receiving services provided by Defendant. Plaintiff and Class Members provided their PII to Defendant or its third-party agents in exchange for Defendant's services.

115. Plaintiff and Class Members reasonably understood that a portion of the funds they paid would be used to pay for adequate cybersecurity measures.

116. Plaintiff and Class Members reasonably understood that Defendant would use adequate cybersecurity measures to protect the PII that they were required to provide based on Defendant's duties under state and federal law and its internal policies.

117. Plaintiff and the Class Members accepted Defendant's offers by disclosing their PII to Defendant or its third-party agents in exchange for services.

118. In turn, and through internal policies, Defendant agreed to protect and not disclose the PII to unauthorized persons.

119. In its Privacy Policy, Defendant represented that it had a legal duty to protect Plaintiff's and Class Member's PII.

120. Implicit in the parties' agreement was that Defendant would provide Plaintiff and Class Members with prompt and adequate notice of all unauthorized access and/or theft of their PII.

121. After all, Plaintiff and Class Members would not have entrusted their PII to Defendant in the absence of such an agreement with Defendant.

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

123. The covenant of good faith and fair dealing is an element of every contract. Thus, parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—and not merely the letter—of the bargain. In short, the parties to a contract are mutually obligated to comply with the substance of their contract in addition to its form.

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

125. Defendant materially breached the contracts it entered with Plaintiff and Class Members by:

- a. failing to safeguard their information;
- b. failing to notify them promptly of the intrusion into its computer systems that compromised such information.

- c. failing to comply with industry standards;
- d. failing to comply with the legal obligations necessarily incorporated into the agreements; and
- e. failing to ensure the confidentiality and integrity of the electronic PII that Defendant created, received, maintained, and transmitted.

126. In these and other ways, Defendant violated its duty of good faith and fair dealing.

127. Defendant's material breaches were the direct and proximate cause of Plaintiff's and Class Members' injuries (as detailed *supra*).

128. And, on information and belief, Plaintiff's PII has already been published—or will be published imminently—by cybercriminals on the Dark Web.

129. Plaintiff and Class Members performed as required under the relevant agreements, or such performance was waived by Defendant's conduct.

FOURTH CAUSE OF ACTION
Invasion of Privacy
(On Behalf of Plaintiff and the Class)

130. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

131. Plaintiff and the Class had a legitimate expectation of privacy regarding their highly sensitive and confidential PII and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

132. Defendant owed a duty to its current and former customers, including Plaintiff and the Class, to keep this information confidential.

133. The unauthorized acquisition (i.e., theft) by a third party of Plaintiff and Class Members' PII is highly offensive to a reasonable person.

134. The intrusion was into a place or thing which was private and entitled to be private. Plaintiff and the Class disclosed their sensitive and confidential information to Defendant, but did so privately, with the intention that their information would be kept confidential and protected from unauthorized disclosure. Plaintiff and the Class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

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

136. Defendant acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

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

138. Acting with knowledge, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiff and the Class.

139. As a proximate result of Defendant's acts and omissions, the private and sensitive PII of Plaintiff and the Class were stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiff and the Class to suffer damages (as detailed *supra*).

140. And, on information and belief, Plaintiff's PII has already been published—or will be published imminently—by cybercriminals on the Dark Web.

141. Unless and until enjoined and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Class since their PII are still maintained by Defendant with their inadequate cybersecurity system and policies.

142. Plaintiff and the Class have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential records. A judgment for monetary damages will not end Defendant's inability to safeguard the PII of Plaintiff and the Class.

143. In addition to injunctive relief, Plaintiff, on behalf of himself and the other Class Members, also seeks compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest and costs.

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

144. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

145. This claim is pleaded in the alternative to the breach of implied contract claim.

146. Plaintiff and Class Members conferred a benefit upon Defendant. After all, Defendant benefitted from (1) using their PII to provide services, and (2) accepting payment.

147. Defendant appreciated or had knowledge of the benefits it received from Plaintiff and Class Members.

148. Plaintiff and Class Members reasonably understood that Defendant would use adequate cybersecurity measures to protect the PII that they were required to provide based on Defendant's duties under state and federal law and its internal policies.

149. Defendant enriched itself by saving the costs they reasonably should have expended on data security measures to secure Plaintiff's and Class Members' PII.

150. Instead of providing a reasonable level of security, or retention policies, that would have prevented the Data Breach, Defendant instead calculated to avoid its 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 the requisite security.

151. Under principles of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiff's and Class Members' (1) PII and (2) payment because Defendant failed to adequately protect their PII.

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

153. Defendant should be compelled to disgorge into a common fund—for the benefit of Plaintiff and Class Members—all unlawful or inequitable proceeds that it received because of its misconduct.

SIXTH CAUSE OF ACTION
Breach of Fiduciary Duty
(On Behalf of Plaintiff and the Class)

154. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

155. Given the relationship between Defendant and Plaintiff and Class Members, where Defendant became guardian of Plaintiff's and Class Members' PII, Defendant became a fiduciary by its undertaking and guardianship of the PII, to act primarily for Plaintiff and Class Members, (1) for the safeguarding of Plaintiff and Class Members' PII; (2) to timely notify Plaintiff and Class Members of a Data Breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendant did and does store.

156. Defendant has a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of Defendant’s relationship with them—especially to secure their PII.

157. Because of the highly sensitive nature of the PII, Plaintiff and Class Members would not have entrusted Defendant, or anyone in Defendant’s position, to retain their PII had they known the reality of Defendant’s inadequate data security practices.

158. Defendant breached its fiduciary duties to Plaintiff and Class Members by failing to sufficiently encrypt or otherwise protect Plaintiff’s and Class Members’ PII.

159. Defendant also breached its fiduciary duties to Plaintiff and Class Members by failing to diligently discover, investigate, and give notice of the Data Breach in a reasonable and practicable period.

160. As a direct and proximate result of Defendant’s breach of its fiduciary duties, Plaintiff and Class Members have suffered and will continue to suffer numerous injuries (as detailed *supra*).

SEVENTH CAUSE OF ACTION
Violation of the New Jersey Consumer Fraud Act
N.J.S.A. §§ 56:8 *et seq.*
(On Behalf of Plaintiff and the Class)

161. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

162. Defendant violated New Jersey Consumer Fraud Act by, *inter alia*:

- a. making material misrepresentations about maintaining Plaintiff’s and the Class’ PII in a private, safe and secure manner;
- b. failing to implement and maintain reasonable security and privacy measures in contravention of its representations to protect Plaintiff’s and Class Members’ PII, which was a direct and proximate cause of the Data Breach;

- c. failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- d. failing to comply with common law, regulatory and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq.*, which was a direct and proximate cause of the Data Breach;
- e. omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Class Members' PII; and
- f. omitting, suppressing, and concealing the material fact that it did not comply with common law, regulatory and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq.*

163. The New Jersey Consumer Fraud Act defines merchandise as “any objects, wares, goods, commodities, services or anything offered, directly or indirectly to the public for sale.” N.J.S.A. § 56:8-1(c).

164. At all relevant times, Defendant advertised and sold goods and services that are merchandise within the meaning of the New Jersey Consumer Fraud Act.

165. Defendant's omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of their PII.

166. Defendant intended to mislead Plaintiff and Class Members and induce them to rely on its omissions.

167. Had Defendant disclosed to Plaintiff and Class Members that its data systems were not secure—and thus vulnerable to attack—Defendant would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Defendant accepted the PII that Plaintiff and Class Members entrusted to it while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff and Class Members acted reasonably in relying on Defendant's omissions, the truth of which they could not have discovered through reasonable investigation.

168. Defendant acted intentionally, knowingly, maliciously, and recklessly disregarded Plaintiff's and Class Members' rights.

167. Under the New Jersey Consumer Fraud Act, the following qualifies as an unlawful practice:

The act, use or employment by any person of any unconscionable commercial practice, deception, fraud, false pretense, false promise, misrepresentation, or the knowing, concealment, suppression, or omission of any material fact with intent that others rely upon such concealment, suppression or omission, in connection with the sale or advertisement of any merchandise or real estate, or with the subsequent performance of such person as aforesaid, whether or not any person has in fact been misled, deceived or damaged thereby.

N.J.S.A. § 56:8-2.

168. In enacting the Identity Theft Prevention Act ("ITPA"), N.J.S.A. 56:8-161 to - 166.3, which among other things, amended the New Jersey Consumer Fraud Act, the New Jersey

Legislature found that “[i]dentity theft is an act that violates the privacy of our citizens and ruins their good names: victims can suffer restricted access to credit and diminished employment opportunities, and may spend years repairing damage to credit histories.” N.J.S.A. § 56:11-45.

169. At all relevant times, Defendant conducted business in New Jersey and collected Private Information from New Jersey residents within the meaning of the ITPA.

170. Defendant violated the ITPA by failing to disclose the Data Breach in the most expedient time possible and without unreasonable delay to: (i) customers, (ii) The New Jersey State Police, and (iii) Consumer Reporting Agencies, in violation of N.J.S.A. 56:8-163(a), N.J.S.A. 56:8-163(c)1, and N.J.S.A. 56:8-163(f).

171. Defendant’s failure to safeguard Private Information and its promises to do so constitutes an unconscionable commercial practice, deception, fraud, false pretense, false promise, or misrepresentation because Defendant knew that it had not adopted adequate electronic or physical safeguards to protect Private Information. More specifically, Plaintiffs allege that Defendant failed to implement and maintain reasonable security practices to protect Private Information, failed to store Private Information in a way that maximized its security and confidentiality, and permitted or failed to prevent the disclosure of Private Information.

172. Plaintiffs and Class Members had a reasonable expectation that their Private Information would be protected and the failure to do so constitutes an unconscionable commercial practice, deception, fraud, false pretense, false promise, or misrepresentation in violation of N.J.S.A. § 56:8-2.

173. Defendant had a duty to advise Plaintiffs and Class Members that its data security was inadequate, and by not doing so, concealed, suppressed, or omitted material facts.

174. Defendant intended for Plaintiffs and the members of the proposed Class to rely upon the concealment, suppression, or omission of material fact relating to its data security.

175. Plaintiffs and Class Members had a reasonable expectation that data security was adequate when they provided their Private Information to Defendant.

176. Plaintiffs and Class Members would not have conducted business with or provided their Private Information as required to Defendant if it had not concealed, suppressed, or omitted the material fact relating to its data security.

177. Defendant's actions constitute a knowing, concealment, suppression, or omission in violation of N.J.S.A. § 56:8-2. As a result of the foregoing, Plaintiffs and Class Members suffered and will continue to suffer ascertainable losses and other damages as described in detail herein and are entitled to treble damages as provided by N.J.S.A. § 56:18-19.

178. Further, Defendant failed to destroy stale records in violation of N.J.S.A. § 56:8-162, which requires that a business “destroy, or arrange for the destruction of, a customer’s records within its custody or control containing personal information, which is no longer to be retained by the business or public entity, by shredding, erasing, or otherwise modifying the personal information in those records to make it unreadable, undecipherable or nonreconstructable through generally available means.” N.J.S.A. § 56:8-162.

179. The New Jersey Consumer Fraud Act provides that it is “an unlawful practice and a violation of P.L. 1960, c. 39 (c. 56:8-1 *et seq.*) to willfully, knowingly or recklessly violate” Sections 56:8-161-164 of that Act.

180. In violation of N.J.S.A. § 56:8-162, Defendant retained its former patients; or customers’ Private Information in an unprotected and insecure manner.

181. There are technologies available and programs that can be implemented that automatically wipe information when an event occurs ending the individual's relationship with the entity at issue. Because Defendant failed to employ any technologies to protect or destroy the Private Information at issue, it has violated § 56:8-162 of the New Jersey Consumer Fraud Act.

182. As a result of the foregoing, Plaintiff and Class Members suffered and will continue to suffer ascertainable losses and other damages as described herein and are entitled to treble damages as provided by N.J.S.A. § 56:18-19.

183. In addition, Defendant failed to expediently notify victims following the Data Breach in violation of the New Jersey Consumer Fraud Act, N.J.S.A. 56:8-2 *et seq.*

184. Section 56:8-163 of the New Jersey Consumer Fraud Act requires that a business conducting business in New Jersey:

shall disclose any breach of security of those computerized records following discovery or notification of the breach to any customer who is a resident of New Jersey whose personal information was, or is reasonably believed to have been, accessed by an unauthorized person. The disclosure to a customer shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subsection c. of this section, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

N.J.S.A. § 56:8-163.

185. The New Jersey Consumer Fraud Act defines a breach of security as follows:

“Breach of security” means unauthorized access to electronic files, media or data containing personal information that compromises the security, confidentiality or integrity of personal information when access to the personal information has not been secured by encryption or by any other method or technology that renders the acquisition of personal information by an employee or agent of the business for a

legitimate business purpose is not a breach of security, provided that the personal information is not used for a purpose unrelated to the business or subject to further unauthorized disclosure.

N.J.S.A. § 56:8-161. The Data Breach constituted a breach of security.

186. Defendant's disclosure regarding the Data Breach to Plaintiffs and Class Members is delayed and not made in the most expedient time possible.

187. As a direct and proximate result of Defendant's unfair and deceptive acts and practices, Plaintiff and Class Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their PII.

188. And, on information and belief, Plaintiff's PII has already been published—or will be published imminently—by cybercriminals on the Dark Web.

189. Plaintiff and Class Members seek all monetary and non-monetary relief allowed by law.

EIGHTH CAUSE OF ACTION
Declaratory Judgment
(On Behalf of Plaintiff and the Class)

190. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

191. 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. The Court has broad authority to restrain acts, such as those alleged herein, which are tortious and unlawful.

192. In the fallout of the Data Breach, an actual controversy has arisen about Defendant's various duties to use reasonable data security. On information and belief, Plaintiff alleges that Defendant's actions were—and *still* are—inadequate and unreasonable. And Plaintiff and Class Members continue to suffer injury from the ongoing threat of fraud and identity theft.

193. Given its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

- a. Defendant owed—and continues to owe—a legal duty to use reasonable data security to secure the data entrusted to it;
- b. Defendant has a duty to notify impacted individuals of the Data Breach under the common law and Section 5 of the FTC Act;
- c. Defendant breached, and continues to breach, its duties by failing to use reasonable measures to the data entrusted to it; and
- d. Defendant breaches of its duties caused—and continues to cause—injuries to Plaintiff and Class Members.

194. The Court should also issue corresponding injunctive relief requiring Defendant to use adequate security consistent with industry standards to protect the data entrusted to it.

195. If an injunction is not issued, Plaintiff and the Class will suffer irreparable injury and lack an adequate legal remedy if Defendant experiences a second data breach.

196. And if a second breach occurs, Plaintiff and the Class will lack an adequate remedy at law because many of the resulting injuries are not readily quantified in full and they will be forced to bring multiple lawsuits to rectify the same conduct. Simply put, monetary damages—while warranted for out-of-pocket damages and other legally quantifiable and provable damages—cannot cover the full extent of Plaintiff and Class Members' injuries.

197. If an injunction is not issued, the resulting hardship to Plaintiff and Class Members far exceeds the minimal hardship that Defendant could experience if an injunction is issued.

198. An injunction would benefit the public by preventing another data breach—thus preventing further injuries to Plaintiff, Class Members, and the public at large.

PRAYER FOR RELIEF

Plaintiff and Class Members respectfully request judgment against Defendant and that the Court enter an order:

- A. Certifying this case as a class action on behalf of Plaintiff and the proposed Class, appointing Plaintiff as class representative, and appointing his counsel to represent the Class;
- B. Awarding declaratory and other equitable relief as necessary to protect the interests of Plaintiff and the Class;
- C. Awarding injunctive relief as necessary to protect the interests of Plaintiff and the Class;
- D. Enjoining Defendant from further unfair and/or deceptive practices;
- E. Awarding Plaintiff and the Class damages including applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;
- F. Awarding restitution and damages to Plaintiff and the Class in an amount to be determined at trial;
- G. Awarding attorneys' fees and costs, as allowed by law;
- H. Awarding prejudgment and post-judgment interest, as provided by law;
- I. Granting Plaintiff and the Class leave to amend this complaint to conform to the evidence produced at trial; and


J. Granting other relief that this Court finds appropriate.

DEMAND FOR JURY TRIAL

Plaintiff demands a jury trial for all claims so triable.

Date: November 25, 2024

Respectfully submitted,

By: 
**KANTROWITZ, GOLDHAMER
& GRAIFMAN, P.C.**
Gary S. Graifman
135 Chestnut Ridge Road
Montvale, New Jersey 07645
Tel: (201) 391-7000
Fax: (201) 307-1086

Samuel J. Strauss*
Raina C. Borrelli*
STRAUSS BORRELLI PLLC
980 N. Michigan Avenue, Suite 1610
Chicago, Illinois 60611
T: (872) 263-1100
F: (872) 263-1109
sam@straussborrelli.com
raina@straussborrelli.com

**Pro hac vice forthcoming
Attorneys for Plaintiff and Proposed Class*

CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. (SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)

I. (a) PLAINTIFFS
JAMIE KEEFER, on behalf of himself
and all others similarly situated,
(b) County of Residence of First Listed Plaintiff Montgomery County, PA
(c) Attorneys (Firm Name, Address, and Telephone Number)
Gary S. Graifman, Esq. ; Kantrowitz, Goldhamer & Graifman, P.C.
135 Chestnut Ridge Road, Suite 200, Montvale, NJ 07645
Tel: 201-391-7000

DEFENDANTS
AMERICAN NEIGHBORHOOD MORTGAGE ACCEPTANCE
COMPANY LLC, DBA ANNIEMAC HOME MORTGAGE
County of Residence of First Listed Defendant Burlington County
NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF
THE TRACT OF LAND INVOLVED.
Attorneys (If Known)

II. BASIS OF JURISDICTION (Place an "X" in One Box Only)
1 U.S. Government Plaintiff
2 U.S. Government Defendant
3 Federal Question (U.S. Government Not a Party)
4 Diversity (Indicate Citizenship of Parties in Item III)

III. CITIZENSHIP OF PRINCIPAL PARTIES (Place an "X" in One Box for Plaintiff and One Box for Defendant)
PTF DEF
Citizen of This State 1 1 Incorporated or Principal Place of Business In This State 4 4
Citizen of Another State 2 2 Incorporated and Principal Place of Business In Another State 5 5
Citizen or Subject of a Foreign Country 3 3 Foreign Nation 6 6

IV. NATURE OF SUIT (Place an "X" in One Box Only) Click here for: Nature of Suit Code Descriptions.

Table with 5 columns: CONTRACT, REAL PROPERTY, TORTS, CIVIL RIGHTS, PRISONER PETITIONS, FORFEITURE/PENALTY, LABOR, IMMIGRATION, BANKRUPTCY, INTELLECTUAL PROPERTY RIGHTS, SOCIAL SECURITY, FEDERAL TAX SUITS, OTHER STATUTES. Includes various legal categories like Insurance, Personal Injury, Real Estate, etc.

V. ORIGIN (Place an "X" in One Box Only)
1 Original Proceeding
2 Removed from State Court
3 Remanded from Appellate Court
4 Reinstated or Reopened
5 Transferred from Another District (specify)
6 Multidistrict Litigation - Transfer
8 Multidistrict Litigation - Direct File

VI. CAUSE OF ACTION
Cite the U.S. Civil Statute under which you are filing (Do not cite jurisdictional statutes unless diversity):
28 U.S.C. § 1332 and 28 U.S.C. § 1332(d); File Pursuant to CAFA
Brief description of cause:
Data Breach of Defendant's computer system.

VII. REQUESTED IN COMPLAINT:
CHECK IF THIS IS A CLASS ACTION UNDER RULE 23, F.R.Cv.P. DEMAND \$ CHECK YES only if demanded in complaint:
JURY DEMAND: Yes No

VIII. RELATED CASE(S) IF ANY (See instructions):
JUDGE Chief Judge Renee Marie Bumb DOCKET NUMBER 1:24-cv-10678

DATE 11/25/2024 SIGNATURE OF ATTORNEY OF RECORD /s/ Gary S. Graifman

FOR OFFICE USE ONLY
RECEIPT # AMOUNT APPLYING IFP JUDGE MAG. JUDGE

INSTRUCTIONS FOR ATTORNEYS COMPLETING CIVIL COVER SHEET FORM JS 44

Authority For Civil Cover Sheet

The JS 44 civil cover sheet and the information contained herein neither replaces nor supplements the filings and service of pleading or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. Consequently, a civil cover sheet is submitted to the Clerk of Court for each civil complaint filed. The attorney filing a case should complete the form as follows:

- I. (a) **Plaintiffs-Defendants.** Enter names (last, first, middle initial) of plaintiff and defendant. If the plaintiff or defendant is a government agency, use only the full name or standard abbreviations. If the plaintiff or defendant is an official within a government agency, identify first the agency and then the official, giving both name and title.
 - (b) **County of Residence.** For each civil case filed, except U.S. plaintiff cases, enter the name of the county where the first listed plaintiff resides at the time of filing. In U.S. plaintiff cases, enter the name of the county in which the first listed defendant resides at the time of filing. (NOTE: In land condemnation cases, the county of residence of the "defendant" is the location of the tract of land involved.)
 - (c) **Attorneys.** Enter the firm name, address, telephone number, and attorney of record. If there are several attorneys, list them on an attachment, noting in this section "(see attachment)".

- II. **Jurisdiction.** The basis of jurisdiction is set forth under Rule 8(a), F.R.Cv.P., which requires that jurisdictions be shown in pleadings. Place an "X" in one of the boxes. If there is more than one basis of jurisdiction, precedence is given in the order shown below.
 - United States plaintiff. (1) Jurisdiction based on 28 U.S.C. 1345 and 1348. Suits by agencies and officers of the United States are included here. United States defendant. (2) When the plaintiff is suing the United States, its officers or agencies, place an "X" in this box.
 - Federal question. (3) This refers to suits under 28 U.S.C. 1331, where jurisdiction arises under the Constitution of the United States, an amendment to the Constitution, an act of Congress or a treaty of the United States. In cases where the U.S. is a party, the U.S. plaintiff or defendant code takes precedence, and box 1 or 2 should be marked.
 - Diversity of citizenship. (4) This refers to suits under 28 U.S.C. 1332, where parties are citizens of different states. When Box 4 is checked, the citizenship of the different parties must be checked. (See Section III below; **NOTE: federal question actions take precedence over diversity cases.**)

- III. **Residence (citizenship) of Principal Parties.** This section of the JS 44 is to be completed if diversity of citizenship was indicated above. Mark this section for each principal party.

- IV. **Nature of Suit.** Place an "X" in the appropriate box. If there are multiple nature of suit codes associated with the case, pick the nature of suit code that is most applicable. Click here for: [Nature of Suit Code Descriptions](#).

- V. **Origin.** Place an "X" in one of the seven boxes.
 - Original Proceedings. (1) Cases which originate in the United States district courts.
 - Removed from State Court. (2) Proceedings initiated in state courts may be removed to the district courts under Title 28 U.S.C., Section 1441.
 - Remanded from Appellate Court. (3) Check this box for cases remanded to the district court for further action. Use the date of remand as the filing date.
 - Reinstated or Reopened. (4) Check this box for cases reinstated or reopened in the district court. Use the reopening date as the filing date.
 - Transferred from Another District. (5) For cases transferred under Title 28 U.S.C. Section 1404(a). Do not use this for within district transfers or multidistrict litigation transfers.
 - Multidistrict Litigation – Transfer. (6) Check this box when a multidistrict case is transferred into the district under authority of Title 28 U.S.C. Section 1407.
 - Multidistrict Litigation – Direct File. (8) Check this box when a multidistrict case is filed in the same district as the Master MDL docket.

PLEASE NOTE THAT THERE IS NOT AN ORIGIN CODE 7. Origin Code 7 was used for historical records and is no longer relevant due to changes in statute.

- VI. **Cause of Action.** Report the civil statute directly related to the cause of action and give a brief description of the cause. **Do not cite jurisdictional statutes unless diversity.** Example: U.S. Civil Statute: 47 USC 553 Brief Description: Unauthorized reception of cable service.

- VII. **Requested in Complaint.** Class Action. Place an "X" in this box if you are filing a class action under Rule 23, F.R.Cv.P.
 - Demand. In this space enter the actual dollar amount being demanded or indicate other demand, such as a preliminary injunction.
 - Jury Demand. Check the appropriate box to indicate whether or not a jury is being demanded.

- VIII. **Related Cases.** This section of the JS 44 is used to reference related cases, if any. If there are related cases, insert the docket numbers and the corresponding judge names for such cases.

Date and Attorney Signature. Date and sign the civil cover sheet.

AO 440 (Rev. 12/09) Summons in a Civil Action

UNITED STATES DISTRICT COURT

for the

District of New Jersey

JAMIE KEEFER, individually, and on behalf of all others similarly situated,

Plaintiff

v.

AMERICAN NEIGHBORHOOD MORTGAGE ACCEPTANCE COMPANY LLC, DBA ANNIEMAC HOME MORTGAGE

Defendant

)
)
)
)
)
)
)

Civil Action No.

SUMMONS IN A CIVIL ACTION

To: (Defendant's name and address)

AMERICAN NEIGHBORHOOD MORTGAGE ACCEPTANCE COMPANY LLC DBA ANNIEMAC HOME MORTGAGE
700 East Gate Drive, Suite 400
Mount Laurel, NJ 08054

A lawsuit has been filed against you.

Within 21 days after service of this summons on you (not counting the day you received it) — or 60 days if you are the United States or a United States agency, or an officer or employee of the United States described in Fed. R. Civ. P. 12 (a)(2) or (3) — you must serve on the plaintiff an answer to the attached complaint or a motion under Rule 12 of the Federal Rules of Civil Procedure. The answer or motion must be served on the plaintiff or plaintiff's attorney, whose name and address are:

Gary S. Graifman, Esq.
Kantrowitz, Goldhamer & Graifman, P.C.
135 Chestnut Ridge Road, Suite 200,
Montvale, NJ 07645
Tel: 201-391-7000

If you fail to respond, judgment by default will be entered against you for the relief demanded in the complaint. You also must file your answer or motion with the court.

CLERK OF COURT

Date: _____

Signature of Clerk or Deputy Clerk

Civil Action No. _____

PROOF OF SERVICE

(This section should not be filed with the court unless required by Fed. R. Civ. P. 4 (l))

This summons for *(name of individual and title, if any)* _____
was received by me on *(date)* _____.

I personally served the summons on the individual at *(place)* _____
_____ on *(date)* _____; or

I left the summons at the individual's residence or usual place of abode with *(name)* _____
_____, a person of suitable age and discretion who resides there,
on *(date)* _____, and mailed a copy to the individual's last known address; or

I served the summons on *(name of individual)* _____, who is
designated by law to accept service of process on behalf of *(name of organization)* _____
_____ on *(date)* _____; or

I returned the summons unexecuted because _____; or

Other *(specify)*: _____

My fees are \$ _____ for travel and \$ _____ for services, for a total of \$ _____ 0.00.

I declare under penalty of perjury that this information is true.

Date: _____

Server's signature

Printed name and title

Server's address

Additional information regarding attempted service, etc: