IN THE CIRCUIT COURT OF JACKSON COUNTY, MISSOURI
AT INDEPENDENCE

JAMES DAILEY, individually and on behalf of all others similarly situated, Plaintiffs, v. BETHESDA FOUNDATION, and AUTUMN VIEW GARDENS, Defendants.	Case No.: **JURY TRIAL DEMANDED**

CLASS ACTION PETITION

Plaintiff James Dailey ("Plaintiff" and/or "Dailey"), by and through his undersigned counsel, bring this Class Action Petition against Defendant Bethesda Foundation ("Bethesda") and Defendant Autumn View Gardens (collectively, "Defendants"), individually and on behalf of all others similarly situated, and allege as follows, based upon personal knowledge as to themselves, and upon information and belief as to all other matters.

INTRODUCTION

1. Bethesda Foundation is the owner and operator of Autumn View Gardens, an assisted living and memory care facility that provides residential care services to elderly and vulnerable individuals. As part of its operations, Bethesda collects, maintains, and stores highly sensitive personal information and protected health information of its residents, patients, their families, and its employees.

2. Between August 19, 2024, and September 18, 2024, Bethesda suffered a data

breach whereby an unauthorized actor gained access to its email system and potentially viewed and/or downloaded emails containing sensitive personal and health information (the "Data Breach"). The compromised information included, at a minimum, names, dates of birth, Social Security numbers, financial account numbers, medical record numbers, Medicare numbers, health insurance information, medical diagnoses, treatment information, clinical information, and prescription information.

3. Despite discovering suspicious activity on or around September 18, 2024, Bethesda failed to timely notify affected individuals of the Data Breach. Bethesda did not send notification letters until February 28, 2025—over five months after discovering the breach—leaving victims vulnerable to identity theft and fraud during this critical period.

4. Individuals impacted by the Data Breach are now at serious risk of continuing injury caused by the exposure of their highly sensitive personal and health information, which remains in the possession of cybercriminals who gained unauthorized access to Bethesda's systems.

5. As a facility entrusted with the care of elderly and vulnerable individuals, many of whom suffer from memory impairments and other health conditions, Bethesda had a heightened duty to protect the sensitive information in its possession. Bethesda's failure to implement adequate security measures and its unconscionable delay in notifying victims represents a fundamental breach of the trust placed in it by residents and their families.

PARTIES

6. Plaintiff James Dailey is a resident and citizen of Kansas City, Missouri.

7. Defendant Bethesda Foundation is a Nebraska nonprofit corporation with its principal place of business located at 15475 Gleneagle Dr., Colorado Springs, Colorado 80921.

Bethesda may be properly served with process by serving its registered agent: CT Corporation System, 5661 Telegraph Rd., Ste. 4B, St. Louis, Missouri 63129.

8. Defendant Autumn View Gardens is a Missouri nonprofit corporation operating under Charter No. X00311499. Autumn View Gardens may be properly served with process through the Missouri Secretary of State, pursuant to Mo. Rev. Stat.§ 355.176, as it does not currently maintain a registered agent for service of process in Missouri.

JURISDICTION & VENUE

9. This Court has subject-matter jurisdiction over this action because Defendants have submitted themselves to the jurisdiction of the courts of this state by transacting business within the state pursuant to RSMo. § 506.500.1

10. Venue is proper in this Court pursuant to Mo. Rev. Stat. § 508.010.4, because Plaintiff resides in Jackson County, Missouri, and a substantial part of the events or omissions giving rise to the claims occurred in Jackson County, Missouri, including Plaintiff's provision of personal information in connection with his workers' compensation claim and Defendants' failure to safeguard such information.

FACTUAL ALLEGATIONS

Autumn View Gardens' Data Management and Privacy Practices

11. Autumn View Gardens is an assisted living and memory care facility that provides residential and healthcare services to elderly residents throughout multiple locations.

12. As part of its operations, Autumn View Gardens collects, stores, and maintains highly sensitive personal and protected health information from its residents, employees, and third parties including workers' compensation claimants.

13. In the course of providing services and managing workers' compensation claims, Autumn View Gardens routinely collects and stores Personal Identifying Information ("PII") and

Protected Health Information ("PHI"), including but not limited to names, dates of birth, Social Security numbers, financial account information, medical record numbers, Medicare numbers, health insurance information, medical diagnoses, treatment information, clinical information, and prescription information.

14. Autumn View Gardens knew, or should have known, that the sensitive nature of the information it collected made it a prime target for cybercriminals seeking to exploit such data for financial gain through identity theft, medical fraud, and other illicit purposes.

15. By obtaining, collecting, and storing PII and PHI, Defendant assumed legal and equitable duties and knew or should have known it was responsible for protecting this data from unauthorized disclosure.

The Data Breach

16. On or around September 18, 2024, Autumn View Gardens identified suspicious activity within its email system.

17. The investigation revealed that an unauthorized actor had gained access to Autumn View Gardens' email system between August 19, 2024 and September 18, 2024.

18. During this period, the unauthorized actor potentially viewed and/or downloaded certain emails containing sensitive personal and protected health information of current and former employees, residents, and individuals involved in workers' compensation claims.

19. The compromised information included highly sensitive data such as names, dates of birth, Social Security numbers, financial account numbers, medical record numbers, Medicare numbers, health insurance information, medical diagnoses, treatment and procedure information, clinical information, prescription information, and healthcare provider information.

20. Despite discovering the breach on or around September 18, 2024, Autumn View Gardens failed to promptly notify affected individuals.

21. Many victims, including Plaintiff, did not receive notification until February 28, 2025—more than five months after the breach was discovered.

22. This unconscionable delay in notification prevented victims from taking timely action to protect themselves from identity theft and fraud, leaving them vulnerable to criminal exploitation of their most sensitive personal and health information.

23. When Autumn View Gardens finally provided notice, it downplayed the severity of the breach, claiming there was "no evidence that your information has been misused," despite the fact that cybercriminals had unfettered access to download and exploit the data over several months.

The Data Breach was Preventable

24. Upon information and belief, the breach resulted from Autumn View Gardens' failure to implement and maintain reasonable and industry-standard security measures to protect the email systems containing sensitive personal and health information.

25. Healthcare facilities and their business associates are well-known targets for cyberattacks due to the valuable nature of the medical and personal information they maintain. Despite this known risk, Autumn View Gardens failed to implement adequate safeguards.

26. Industry-standard security measures that could have prevented or mitigated this breach include:

a. Multi-factor authentication for email access

b. Email encryption for sensitive data

c. Regular security audits and penetration testing

d. Employee training on phishing and social engineering attacks

e. Advanced email filtering and threat detection systems

f. Network segmentation to limit access to sensitive data

g. Timely patching and updating of systems

27. Upon information and belief, by implementing enhanced security measures only after the breach occurred, Autumn View Gardens demonstrated that it had previously failed to maintain reasonable data security practices despite its knowledge of the risks.

The Effects of the Data Breach on Impacted Individuals

28. As a direct and proximate result of the Data Breach, Plaintiff and Class members have been exposed to a substantially increased risk of identity theft, medical identity theft, financial fraud, and other identity-related crimes.

29. The unauthorized access to medical information creates particular risks, as medical identity theft can result in fraudulent insurance claims, incorrect medical records, and potentially life-threatening medical errors when fraudulent information becomes part of a victim's permanent medical record.

30. The combination of Social Security numbers with medical and financial information provides criminals with a complete profile to commit sophisticated identity theft schemes that can persist for years or even decades.

31. Plaintiff and Class members must now vigilantly monitor their financial accounts, credit reports, medical records, insurance statements, and tax filings indefinitely to detect fraudulent activity.

32. The unauthorized disclosure of sensitive PII and PHI to data thieves also reduces the value of that information to its rightful owner, which has been recognized as an independent

form of harm. Plaintiff and the Class members had, and continue to have, a protectible property interest in their PII and PHI.

33. Plaintiff and the Class members seek to recover the value of the unauthorized access to their PII and PHI permitted by Defendants' wrongful conduct. This measure of damages is analogous to the remedies for unauthorized use of intellectual property. Like a technology covered by a trade secret or patent, use of or access to a person's PII and PHI is non-rivalrous — the unauthorized use by another does not diminish the rights-holder's own ability to use that information.

34. Nevertheless, a plaintiff may generally recover the reasonable-use value of such property — i.e., a "reasonable royalty" — from an infringer. This is true even where the unauthorized use did not interfere with the owner's own use of the property and even where the owner would not have otherwise licensed or transferred such information to the infringer.

35. A similar royalty or license measure of damages is appropriate here under common-law damages principles authorizing recovery of rental or use value. This measure is appropriate because: (a) Plaintiff and the Class members have a protectible property interest in their PII and PHI; (b) the minimum damages measure for the unauthorized use of personal property is its rental value; and (c) that rental value is established with reference to market value — i.e., based on evidence as to the value of similar transactions in the data marketplace.

ALLEGATIONS RELATING TO PLAINTIFF JAMES DAILEY

36. Plaintiff James Dailey is a resident and citizen of Kansas City, Missouri.

37. In 2019, while working for Bethesda, Plaintiff suffered a head and neck injury that resulted in a workers' compensation claim.

38. As part of this claim, Plaintiff was required to provide extensive personal, financial, and medical information to Bethesda, which handled aspects of the workers' compensation process.

39. The information Plaintiff provided included his full name, date of birth, Social Security number, financial account information, detailed medical records related to his injury, medical diagnoses, treatment information, and health insurance information.

40. Plaintiff's workers' compensation case remained open through, at least, August to September 2024, during which time his sensitive information remained in Autumn View Gardens' possession and was exposed during the Data Breach.

41. Despite the breach occurring in the August to September 2024 time-frame, Plaintiff did not receive notification until February 28, 2025—approximately five to six months after the unauthorized access began.

42. The February 28, 2025 notice letters Plaintiff received confirmed that an unauthorized actor had gained access to Autumn View Gardens' network system and potentially downloaded his personal information, including his date of birth, Social Security number, financial account information, medical record number, Medicare number, health insurance information, medical diagnosis information, medical treatment information, clinical information, prescription information, and healthcare provider information.

43. The extensive list of compromised data matched exactly the categories of information Plaintiff had provided in connection with his workers' compensation claim, confirming that his most sensitive personal and medical information had been exposed.

44. When Plaintiff contacted the breach hotline seeking answers, he received only boilerplate responses that were limited to the information in the letter.

45. The representative could not confirm what specific information was stolen, claimed there was "no evidence of adverse effects," and refused to accept responsibility for the breach.

46. As a result of the Data Breach and Autumn View Gardens' delayed notification, Plaintiff has expended and continues to expend significant time and effort monitoring his accounts, investigating the breach, searching for legal representation, and taking steps to protect himself from identity theft.

47. Plaintiff has experienced significant stress, anxiety, and frustration as a result of the breach, particularly given the highly sensitive nature of the medical and financial information exposed and the lack of transparency from Autumn View Gardens.

48. Due to the nature of the information compromised—including the unique combination of his Social Security number, medical information, and financial data—Plaintiff faces a substantial and imminent risk of identity theft, medical identity theft, tax fraud, and financial fraud for the rest of his life.

49. Plaintiff has been damaged by Defendants' negligent handling of his sensitive information and continues to suffer harm from the ongoing risk of identity theft and the time and effort required to monitor and protect his accounts indefinitely.

CLASS ACTION ALLEGATIONS

50. Plaintiff brings this action on behalf of himself, and all other persons similarly situated, pursuant to Missouri Rule of Civil Procedure 52.08.

51. Plaintiff proposes that he represent all persons who meet the following definition (the "Class"):

> ***All former and current employees and independent contractors of Bethesda Foundation and/or Autumn View Gardens whose personally identifiable information ("PII") and/or protected health information ("PHI") was exposed during the Data Breach.***

52. Plaintiff reserves the right to amend the foregoing class definition and/or to define sub-classes before this Court determines whether certification is appropriate.

53. Excluded from the Class are (a) all Missouri state-court judges and members of their families within the first degree of consanguinity, (b) Defendants' officers and directors and counsel of record, and (c) any state or political subdivisions of a state.

54. **Numerosity:** Upon information and belief, the proposed class would compromise at least 650 individuals. Bethesda was, per its website, founded in 1974. Given the current number of employees and relatively high natural turnover in the labor market, it's likely that the personal information of thousands of *former* employees and/or independent contractors was compromised during the breach. Additionally, according to the Missouri Long Term Care Facilities Directory, Autumn View Gardens possesses a capacity of one hundred and fifty (150) beds at their Ellisville, Missouri location and one hundred and ten (110) beds at their Creve Coeur, Missouri location.

55. **Commonality**. This case presents material questions of law and fact common to the Class. Such questions include, but are not limited to:

a. Whether Defendants suffered a data breach that involved Class members' PII and PHI;
b. Whether Class members' Social Security numbers were compromised during the Data Breach;
c. Whether Class members' financial account information was compromised during the Data Breach;
d. Whether Class members' protected health information, including medical diagnoses, treatment information, and prescription data, was compromised during the Data Breach;
e. Whether Defendants provided notice of the Data Breach to Class members within a reasonable amount of time;
f. Whether Defendants' five-to-six-month delay in notifying Class members was unreasonable as a matter of law;
g. Whether Defendants owed Class members a duty of reasonable care in safeguarding their personal and health information;

h. Whether Defendants were negligent in failing to implement adequate security measures to prevent the Data Breach;
i. Whether Defendants owed Class members a duty to promptly notify them of the Data Breach upon discovery;
j. Whether Defendants were negligent in failing to timely notify Class members of the Data Breach;
k. Whether Defendants had an implied contract with Class members to reasonably safeguard their personal and health information;
l. Whether Defendants breached their implied contract with Class members by failing to reasonably safeguard their personal and health information;
m. Whether Defendants had an implied contract with Class members to provide timely notification of any data security incident affecting their information;
n. Whether Defendants breached their implied contract with Class members by waiting over five months to notify them of the Data Breach;
o. Whether Defendants violated HIPAA's Breach Notification Rule by failing to provide timely notice;
p. Whether Defendants acted with reckless disregard for Class members' rights by delaying notification of the Data Breach;
q. Whether Class members sustained damages as a result of Defendants' negligence;
r. Whether Class members sustained damages as a result of Defendants' breach of implied contract;
s. Whether Class members are entitled to injunctive relief requiring Defendants to implement adequate data security measures; and
t. Whether Class members are entitled to credit monitoring and identity theft protection services beyond the inadequate 12-month period offered by Defendants.

56. **Typicality.** Plaintiff's claims are typical of the Class members' claims. The rights of Plaintiff and the other Class members were violated in a virtually identical manner as a direct and/or proximate result of Defendants' willful, reckless and/or negligent actions and/or inaction as to the data breach. Further, all such claims:

a. Present the same elements and burden of proof;

b. Rely upon Defendants' same course of conduct;

c. Rely upon the same legal arguments; and

d. Rely upon the same methods to measure damages.

57. **Adequacy.** Plaintiff and the undersigned counsel are adequate to represent the Class. Plaintiff will fairly and adequately protect the interests of the Class and Plaintiff's counsel are qualified, experienced class-action lawyers who are able to devote the time and resources necessary to represent Plaintiff and the Class.

58. **Predominance.** The questions of law and fact common to the Class members predominate over any questions affecting only individual Class members. Defendants' course of conduct will be discovered without any need for participation by individual Class members.

59. **Superiority.** A class action is superior to all other available methods for the fair and efficient adjudication of this controversy. This action presents textbook facts and circumstances for the certification of a class action so as to afford each individual Class member a fair and efficient manner by which to prosecute their common claims and, likewise, a fair and efficient manner by which Defendants may defend such claims.

60. **Individual Control.** The interests of individual Class members are best served by certifying this case as a class action. Class members' individual actual damages may be relatively small. By contrast, the undersigned counsel believe they will be compelled to invest hundreds of thousands, if not millions, of dollars in time, costs, and expenses in prosecution of this action in order to best prosecute (and win) these Class claims. If counsel represented only Plaintiff, counsel would nevertheless be compelled to expend substantially the same time, costs, and expenses in the prosecution of this action on behalf of Plaintiff, individually. That is, a class action presents desirable economies of scale in litigating this matter.

61. This Court will not experience any material difficulties in its management of this matter as a class action.

COUNT I
NEGLIGENCE

On Behalf of Plaintiff and All Class Members

62. Plaintiff incorporates here by reference all previous paragraphs as though fully set forth herein.

63. Plaintiff and the Class members, as part of their employment, residency, workers' compensation claims, and/or other relationships with Defendants, provided Defendants sensitive personal and health information.

64. Defendants owed a duty to Plaintiff and all Class members to safeguard and protect their sensitive personal and health information, including Social Security numbers, financial account information, and protected health information.

65. Defendants breached that duty by failing to exercise reasonable care in safeguarding Plaintiff's and the other Class members' personal and health information.

66. Defendants also owed Plaintiff and the Class members a duty of care to inform them of the Data Breach and theft of their personal and health information within a reasonable amount of time of ascertaining the same.

67. It was reasonably foreseeable that Defendants' failure to exercise reasonable care in safeguarding Plaintiff's and the other Class members' personal and health information would result in an unauthorized third-party gaining access to such information without a lawful purpose.

68. It was reasonably foreseeable that Defendants' failure to exercise reasonable care in notifying Plaintiff and the Class members as to the theft of their personal and health information would handicap their ability to mitigate damages from that theft.

69. Plaintiff and the other Class members suffered, are reasonably certain to continue to suffer, and/or are reasonably certain to suffer damages as a direct and proximate result of Defendants' failure to secure their personal and health information and notify them of the breach.

Such damages may come in forms including, but not limited to: expenses for credit monitoring; identity-theft insurance; out-of-pocket expenses; invasion of privacy; lost or delayed tax refunds; wasted time; diminution in the value of their personal and health information; risk of medical identity theft; compensation for the reasonable-use value of the PII; and emotional distress, all of which entitles Plaintiff and the Class members to compensation.

70. Defendants' wrongful actions and/or inactions as to prevention and notice of the data breach entailed, and continue to entail, negligence under the common law.

COUNT II
NEGLIGENCE PER SE
On Behalf of Plaintiff and All Class Members

71. Plaintiff incorporates here by reference all previous paragraphs as though fully set forth herein.

72. Section 5 of the FTC Act prohibits "unfair…practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendants, of failing to use reasonable measures to protect PII. *See* 15 U.S.C. § 45(a)(1).

73. Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to protect Plaintiffs and the Class members' PII and by failing to comply with applicable industry standards. Defendant's conduct was particularly unreasonable given the sensitive nature of the PII it obtained and stored.

74. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se*.

75. Plaintiffs and the Class members are within the class of persons that the FTC Act was intended to protect.

76. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses

that, as a result of their failure to employ reasonable data security measures, caused the same type of harm as that suffered by Plaintiffs and the Class.

77. As a direct and proximate result of Defendants negligence *per se*, Plaintiffs and the Class members have suffered, and will continue to suffer, injuries, damages, and ahrm as described herein.

COUNT III
BREACH OF IMPLIED CONTRACT
On Behalf of Plaintiffs and All Class Members

78. Plaintiff incorporates here by reference all previous paragraphs as though fully set forth herein.

79. Plaintiff and the Class members, as part of their employment, residency, workers' compensation claims, and/or other relationships with Defendants, provided Defendants sensitive personal and health information.

80. In providing such personal and health information, Plaintiff and the other members of the Class entered an implied contract with Defendants, whereby Defendants became obligated to reasonably safeguard their personal and health information.

81. Under that implied contract, Defendants were obligated to not only safeguard that personal and health information but also to provide Plaintiff and the Class members with prompt, adequate notice of any data breach or otherwise unauthorized access of said information.

82. Defendants breached the implied contract with Plaintiff and the other Class members by failing to take reasonable measures to safeguard their personal and health information.

83. Defendants also breached the contract with Plaintiff and the other Class members by failing to provide them prompt, adequate notice of the Data Breach.

84. This breach of implied contract occurred under the common law.

85. Defendants acted with reckless disregard as to Plaintiff's rights, and the rights of the Class members, when they failed to timely inform them that their personal and health information was compromised in the Data Breach.

86. Plaintiff and the other Class members suffered, are reasonably certain to continue to suffer, and/or are reasonably certain to suffer damages as a direct and proximate result of Defendants' failure to secure their personal and health information and notify them of the breach. Such damages may come in forms including, but not limited to: the reasonable-use value of the unauthorized access to Plaintiff's and the Class members' PII and PHI; expenses for credit monitoring; identity-theft insurance; out-of-pocket expenses; invasion of privacy; lost or delayed tax refunds; wasted time; diminution in the value of their personal and health information; risk of medical identity theft; and emotional distress, all of which entitles Plaintiff and the Class members to compensation.

COUNT IV
BREACH OF CONFIDENCE
On Behalf of Plaintiffs and All Class Members

87. Plaintiff incorporates here by reference all previous paragraphs as though fully set forth herein.

88. Plaintiff and the Class members maintained a confidential relationship with Defendants whereby Defendants assumed a duty to not disclose the PII and PHI to unauthorized third parties. The PII and PHI was confidential, novel, highly personal, and sensitive.

89. Defendants knew Plaintiff and the Class members' PII and PHI was being disclosed in confidence and understood the confidence was to be maintained, including by expressly and implicitly agreeing to protect the confidentiality and security of the PII and PHI they collected, stored, and maintained.

90. The Data Breach comprised unauthorized disclosure of Plaintiff and the Class members' PII and PHI, in violation of this understanding.

91. This non-consensual disclosure occurred because Defendants failed to implement and maintain reasonable safeguards to protect the PII and PHI in their possession. Defendants' recklessness in failing to comply with industry-standard data security practices amounted to intentional behavior.

92. Plaintiff and the Class members suffered harm the moment the unauthorized disclosure of the PII and PHI to a third party occurred.

93. As a direct and proximate result of Defendants' breach of confidence, Plaintiff and the Class members suffered injury and sustained actual losses and damages, including but not limited to the reasonable-use value of the unauthorized access to their PII and PHI, as alleged herein. Plaintiff and the Class members alternatively seek an award of nominal damages.

COUNT V
BREACH OF FIDUCIARY DUTY
On Behalf of Plaintiffs and All Class Members

94. Plaintiff incorporates here by reference all previous paragraphs as though fully set forth herein.

95. A fiduciary relationship existed between Defendants and Plaintiff and the Class members.

96. Plaintiff and the Class members placed Defendants in a position of trust and confidence by providing them with the PII and PHI as a condition of their employment, residency, workers' compensation claims, or other relationships, which PII and PHI was accepted and appreciated by Defendants.

97. Defendants assumed a duty not to disclose the PII and PHI provided by Plaintiff and the Class members to unauthorized third parties.

98. Again, the PII and PHI was confidential, novel, highly personal, and sensitive.

99. Defendants breached the fiduciary duty owed to Plaintiff and the Class members by failing to act with the utmost good faith, fairness, and honesty, and failing to protect the PII and PHI in their possession.

100. As a direct and proximate result of Defendants' breach of fiduciary duty, Plaintiff and the Class members suffered injury and sustained actual losses and damages, as described herein. Plaintiff and the Class members alternatively seek an award of nominal damages.

COUNT VI
FRAUDULENT CONCEALMENT
On Behalf of Plaintiffs and All Class Members

101. Plaintiff incorporates here by reference all previous paragraphs as though fully set forth herein.

102. Defendants had knowledge of the Data Breach by September 18, 2024, including the knowledge that Plaintiff and the Class members were at significant risk of identity theft and related fraud, which they could not otherwise have known or discovered through the existence of reasonable diligence.

103. Defendants had legal and equitable duties to disclose the Data Breach to Plaintiff and the Class members within a reasonable timeframe after they learned, or should have known, of the breach.

104. Defendants deliberately failed to communicate this information to Plaintiff and the Class members, attempting to conceal the existence of the Data Breach and attendant risks of harm associated with it.

105. Plaintiff and the Class members justifiably relied on Defendants to communicate the existence of the Data Breach and attendant risks of harm associated with it.

106. Plaintiff and the Class members were injured by Defendants' failure to communicate this information as they were unable to take actions to prevent and/or mitigate the harms of identity theft and related fraud before they occurred.

107. As a direct and proximate result of Defendants' fraudulent concealment, Plaintiff and the Class members suffered injury and sustained actual losses and damages, as described herein. Plaintiff and the Class members alternatively seek an award of nominal damages.

COUNT VII
DECLARATORY JUDGMENT
On Behalf of Plaintiffs and All Class Members

108. Plaintiff incorporates here by reference all previous paragraphs as though fully set forth herein.

109. This Court is authorized to enter a judgment declaring the rights and legal relations of the parties and to grant further necessary relief. RSMo §§ 527.010, *et seq.* Furthermore, the Court has broad authority to restrain acts, such as those described herein, that are tortious and violate the terms of the state statutes described in this Class Action Petition.

110. An actual controversy has arisen in the wake of the Data Breach given Defendants' present and prospective duties under the common law, and other sources of law, to reasonably safeguard the PII and PHI of Plaintiff and the Class members.

111. Defendants' misconduct, as described herein, gives rise to a genuine question as to whether Defendants are currently maintaining data-security measures adequate to protect Plaintiff and the Class members from further cyberattacks that could compromise their PII and PHI.

112. Defendants still possess the PII and PHI of Plaintiff and the Class members, which means it remains at risk of further breach because Defendants' data-security measures remain inadequate. Plaintiff and the Class members continue to suffer injuries as a result of the unauthorized access to their PII and PHI and remain at an imminent risk that further such compromises will occur in the future.

113. Pursuant to RSMo §§ 527.010, *et seq.*, Plaintiff seeks a declaration that: (a) Defendants' existing data-security measures do not satisfy their obligations and duties of care; and (b) in order to comply with their obligations and duties of care, Defendants must: (i) purge, delete, or destroy, in a reasonably secure manner, Plaintiff's and the Class members' PII and PHI if such information is no longer necessary to perform essential business functions, so that it is not subject to further unauthorized access or theft; and (ii) implement and maintain reasonable, industry-standard security measures, including, but not limited to:

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

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

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

d. encryption and segmentation of the PII and PHI by, among other things, the creation of firewalls and access controls such that, if one area of Defendants' systems is compromised, hackers cannot gain access to other portions of the system;

e. purging, deleting, and destroying, in a reasonable and secure manner, PII and PHI not necessary to perform essential business functions;

f. conducting regular database scans and security checks;

g. conducting regular employee education regarding best security practices, including awareness training on phishing and social engineering attacks targeting email systems;

h. implementation of multi-factor authentication and the principle of least privilege to combat system-wide cyberattacks; and

i. conducting routine, continuous internal training and education to inform internal security personnel how to identify, manage, and contain a breach.

PRAYER FOR RELIEF

114. WHEREFORE, Plaintiff, on behalf of himself and all Class members, prays for the following relief:

a. An Order certifying the Class as requested herein, designating Plaintiff as Class representative and appointing Plaintiff's counsel as lead counsel for the Class;

b. Judgment entered in favor of Plaintiff and all Class members and against Defendants in an amount that is fair and reasonable as determined by a jury at trial;

c. A declaration that Defendants' existing data-security measures do not satisfy their obligations and duties of care with respect to the PII and PHI of Plaintiff and the Class members that remain in Defendants' custody and control;

d. Equitable and injunctive relief compelling Defendants to: (i) purge, delete, or destroy, in a reasonably secure manner, Plaintiff's and the Class members' PII and PHI that is no longer necessary to perform essential business functions; and (ii) implement and maintain reasonable, industry-standard data security measures as set forth in Count VII above;

e. Pre- and post-judgment interest at the maximum rate permitted by applicable law;

f. All costs incurred in connection with this action; and

g. Such other relief, at law or in equity, as this Court deems just and proper.

DEMAND FOR JURY TRIAL

115. Plaintiff, on behalf of himself and the other Class members, respectfully demands a trial by jury on all claims and causes of action so triable.

Dated: May 13, 2026

Respectfully submitted,

/s/ Bryce B. Bell

Bryce B. Bell MO# 66841
BELL LAW, LLC
2600 Grand Blvd., Suite 580
Kansas City, Missouri 64108
T: 816-886-8206
F: 816-817-8500
Bryce@BellLawKC.com
ATTORNEY FOR PLAINTIFF AND THE PROPOSED CLASS