Exhibit A

IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF TENNESSEE

IN RE AMERICAN RENAL MANAGEMENT LLC DATA BREACH LITIGATION	Case No. 3:25-cv-00248 Class Action Jury Demand District Judge Eli J. Richardson Magistrate Judge Luke A. Evans

CONSOLIDATED CLASS ACTION COMPLAINT

Plaintiffs Pamela Futrell-Parham, Steevenson Jolicoeur, Jhovanna Salazar, Jane Doe, and John Doe, individually and on behalf of all others similarly situated, by and through undersigned counsel, bring this Consolidated Class Action Complaint against Defendant American Renal Management LLC d/b/a Innovative Renal Care ("IRC" or "Defendant"), and allege, upon personal knowledge as to their own acts and experiences and, as to all other matters, upon information and belief based upon the investigation of counsel, as follows.

I. NATURE OF ACTION

1. This is a consolidated class action arising from Defendant's failure to protect and safeguard highly sensitive personally identifiable information ("PII") and protected health information ("PHI") (together, "Private Information") entrusted to Defendant by its current and former employees and patients.

2. Defendant is a "comprehensive kidney care company" with "nearly 250 dialysis centers, over 400 affiliated nephrologists, and a vast network of health system partnerships".[1]

[1] *About*, INNOVATIVE RENAL CARE, https://innovativerenal.com/patient/ (last visited April 08, 2026).

3. As part of its business operations, Defendant collected, received, stored, and maintained the Private Information of thousands of current and former employees and patients, including Plaintiffs and members of the proposed Classes.

4. On or about February 29, 2024, Defendant detected suspicious activity within its computer environment and later determined that an unauthorized actor accessed certain computer systems between February 21, 2024 and March 1, 2024 (the "Data Breach").

5. During that period, the unauthorized actor accessed and copied files from Defendant's internal systems containing Plaintiffs' and Class Members' Private Information.

6. The Private Information compromised in the Data Breach included, upon information and belief, names, addresses, dates of birth, phone numbers, Social Security numbers, driver's license numbers or other state identification numbers, financial account information, taxpayer identification numbers, electronic signatures, health insurance information, medical billing and claim information, medical diagnosis or condition information, medical prescription information, medical record numbers, medical treatment information, patient account numbers, and patient identification numbers.

7. Defendant learned of the Data Breach in or around late February 2024, yet did not begin notifying affected individuals until February 14, 2025, nearly a year later.

8. Defendant's delay in notifying affected individuals deprived Plaintiffs and Class Members of the opportunity to take timely steps to protect themselves from identity theft, fraud, and misuse of their Private Information.

9. Defendant failed to implement reasonable data security safeguards, failed to adequately monitor its systems for unauthorized access, failed to timely detect and contain the

intrusion, failed to adequately train its employees in cybersecurity practices, and failed to provide prompt and adequate notice after discovering the Data Breach.

10. As a direct and proximate result of Defendant's acts and omissions, Plaintiffs' and Class Members' Private Information was exposed to unauthorized third parties and remains at present and continuing risk of misuse.

11. Plaintiffs and Class Members have suffered and will continue to suffer injuries and damages, including but not limited to invasion of privacy, lost or diminished value of their Private Information, out-of-pocket losses, lost time spent monitoring and protecting their identities and accounts, emotional distress, and an increased risk of fraud, identity theft, and medical or financial misuse.

II. PARTIES

12. Plaintiff Pamela Futrell-Parham is a natural person and citizen of the Commonwealth of Virginia, residing in Norfolk, Virginia. At all relevant times, Plaintiff Futrell-Parham was an employee of Defendant and received notice of the Data Breach dated February 14, 2025.

13. Plaintiff Steevenson Jolicoeur is a natural person and citizen of the State of Florida. Plaintiff Jolicoeur received healthcare services from Defendant and, as a condition of receiving those services, provided Defendant with his Private Information.

14. Plaintiff Jhovanna Salazar is a natural person and citizen of the State of California. Plaintiff Salazar entrusted her Personal Information to Defendant in connection with her employment and received a notice letter from Defendant dated February 14, 2025 informing her that her Social Security number was exposed in the Data Breach.

15. Plaintiff Jane Doe is a natural person and citizen of the State of Indiana, residing in Hammond, Indiana. Plaintiff Jane Doe is an employee of Defendant and received a notice of the Data Breach in February 2025.

16. Plaintiff John Doe is a natural person and citizen of the State of Indiana, residing in Whiting, Indiana. Plaintiff John Doe is a current employee of Defendant and received a notice of the Data Breach in February 2025.

17. Defendant American Renal Management LLC d/b/a Innovative Renal Care is a Delaware limited liability company or other business entity organized under Delaware law, with its headquarters and principal executive offices in Franklin, Tennessee, and substantial business operations throughout this District and the United States. Defendant may be served through its registered agent for service of process.

III. JURISDICTION AND VENUE

18. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1332(d)(2), the Class Action Fairness Act, because this is a class action in which the amount in controversy exceeds $5,000,000, exclusive of interest and costs, at least one Class Member is a citizen of a state different from Defendant, and the proposed Classes contain more than 100 members in the aggregate.

19. This Court has personal jurisdiction over Defendant because Defendant is headquartered in this District, regularly conducts business in this District, purposefully avails itself of the privilege of conducting activities in this District, and the acts and omissions giving rise to Plaintiffs' claims occurred in or emanated from this District.

20. Venue is proper in this District pursuant to 28 U.S.C. § 1391 because Defendant is headquartered in this District, a substantial part of the events and omissions giving rise to the claims occurred in this District, and Defendant conducts substantial business in this District.

IV. FACTUAL ALLEGATIONS

A. Defendant's Business and Its Collection of Private Information

21. Defendant is a kidney care company that provides renal treatment and related services and employs individuals in connection with those operations throughout the United States.

22. In the ordinary course of its business, Defendant collected, received, and stored highly sensitive Private Information belonging to its patients and current and former employees.

23. Plaintiffs and Class Members provided their Private Information to Defendant with the reasonable expectation and mutual understanding that Defendant would maintain that information in confidence and protect it from unauthorized access, acquisition, disclosure, and misuse.

24. Defendant derived economic benefit from collecting and maintaining Plaintiffs' and Class Members' Private Information and assumed duties to protect that information through reasonable administrative, technical, and physical safeguards.

25. Defendant knew or should have known that the Private Information entrusted to it was highly valuable to cybercriminals and that any failure to adequately protect that information would create a serious risk of identity theft, financial fraud, medical fraud, and other misuse.

26. Defendant also knew or should have known that its employees and patients would suffer substantial harm if their Private Information were accessed by unauthorized persons.

27. Defendant further recognized these duties, promising in its "Applicant Privacy Notice:"

a. "[IRC] understands and appreciates the importance of personal privacy;"

b. "We follow industry standards and best practices to safeguard the Personal Data we collect;"

c. "These precautions are intended to help prevent unauthorized access, maintain data accuracy, and ensure correct use of information."[2]

B. Defendant's Data Breach

28. On February 29, 2024, Defendant "learned of suspicious activity within certain computer systems."[3]

29. Defendant's investigation revealed that an unauthorized actor accessed its systems between February 21, 2024 and March 1, 2024.[4] Thus, cybercriminals had unfettered access to Defendant's systems, and the files stored therein, for an entire *ten days*. [5]

30. In other words, Defendant's cyber and data security systems were so completely inadequate that it not only allowed cybercriminals to obtain files containing a treasure trove of thousands of its employees' highly private PII but failed to even identify malicious activity before it was too late.

31. Indeed, because the hackers were able to infiltrate Defendant's information systems, located valuable data, and exfiltrate it apparently before Defendant even realized anything was happening, it is likely that Defendant failed to implement basic technical controls like intrusion detection, data loss prevention tools, and endpoint detection and response systems or

---

[2] Privacy Notice, Innovative Renal Care, https://careers.innovativerenal.com/us/en/applicant-privacy-policy (last visited April 8, 2026).

[3] [3] Notice of Data Breach Letter received by Plaintiff Futrell-Parham dated February 14, 2025, a true and correct copy of which is attached hereto as Exhibit A. Defendant sent similar notice letters to the other named Plaintiffs and, upon information and belief, other Class Members.

[4] *Id*.

[5] *Id*.

otherwise failed to implement a centralized alerting system to notify cybersecurity staff when such tools identified malicious or anomalous activity.

32. Defendant's Data Breach compromised personal data collected from employees, including: name, address, date of birth, Social Security number, driver's license or state identification number, financial account information, taxpayer identification number, electronic signature, health insurance information, medical billing/claim information, medical diagnosis or condition information, medical prescription information, medical record number, medical treatment information, patient account number, and patient identification number.[6]

33. Upon information and belief, the Data Breach affected thousands of current and former employees and patients of Defendant.

34. Defendant did not begin issuing notice letters to affected individuals until February 14, 2025, despite having discovered suspicious activity and begun its investigation in February 2024.[7]

35. Thus, Defendant's notice was untimely and inadequate, and failed to provide affected individuals with the prompt information needed to protect themselves from misuse of their Private Information.

36. In Tennessee, companies have an obligation to notify affected individuals within forty-five days of discovery of the breach. Tenn. Code Ann. § 47-18-2107(b).

37. That Defendant blew past this deadline several times over establishes that it almost certainly failed to implement and test a reasonable cybersecurity incident response plan—an elementary administrative safeguard required by every cybersecurity regulatory framework,

[6] Notice of Data Security Event, IRC, (last visited April 8, 2026).

[7] Ex. A.

standard, and guideline, and which are specifically designed to help companies respond to data breaches effectively and in compliance with their notice obligations.

38. Defendant's failure to implement even the most basic safeguards strongly implies the more advanced safeguards fared no better.

39. When Defendant did notify Plaintiffs 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 Plaintiffs and the Class:

a. "remain vigilant against incidents of identity theft and fraud, to review account statements, and to monitor their credit reports and explanation of benefits forms for suspicious activity and to detect errors."[8]

C. Defendant's Failure to Adequately Protect Private Information.

40. Defendant had duties under common law, industry standards, and its own representations and practices to use reasonable measures to protect Plaintiffs' and Class Members' Private Information.

41. Those duties included, among other things, maintaining adequate cybersecurity safeguards, monitoring systems for suspicious activity, detecting intrusions in a timely manner, preventing unauthorized access, training employees in proper cybersecurity practices, and providing prompt notice when a breach occurred.

42. Defendant breached these duties by failing to implement and maintain reasonable security procedures and practices appropriate to the nature of the Private Information it collected and stored.

[8] *Id.*

43. Defendant further breached these duties by failing to adequately monitor its systems, failing to detect the intrusion sooner, failing to prevent unauthorized access to highly sensitive information, and failing to timely notify Plaintiffs and Class Members after discovering the Data Breach.

44. The Data Breach was a foreseeable and preventable consequence of Defendant's inadequate data security practices.

45. Had Defendant implemented reasonable cybersecurity measures, the Data Breach would have been prevented or detected sooner, and the resulting harm to Plaintiffs and Class Members could have been avoided or substantially mitigated.

46. As a direct and proximate result of Defendant's failures, cybercriminals obtained access to Plaintiffs' and Class Members' Private Information, exposing them to present, imminent, and ongoing harm.

D. Defendant Knew, or Should Have Known of the Risk of a Data Breach

47. Upon information and belief, the cybercriminals in question are particularly sophisticated. After all, the cybercriminals defeated the relevant data security systems and gained actual access to sensitive data.

48. 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."[9]

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

[9] 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.

50. It is well known that PII, including Social Security numbers, is an invaluable commodity and a frequent target of hackers.

51. In 2021, there were a record 1,862 data breaches, surpassing both 2020's total of 1,108 and the previous record of 1,506 set in 2017.[10]

52. In light of recent high profile data breaches, including, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Defendant knew or should have known that its electronic records would be targeted by cybercriminals.

53. Indeed, cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets, so they are aware of and take appropriate measures to prepare for and are able to thwart such an attack.

54. Despite the prevalence of public announcements of data breach and data security compromises, and despite its own acknowledgments of data security compromises, and despite its own acknowledgment of its duties to keep PII private and secure, Defendant failed to take appropriate steps to protect the PII of Plaintiffs and Class Members from being compromised.

55. In the years immediately preceding the Data Breach, Defendant knew or should have known that Defendant's computer systems were a target for cybersecurity attacks, including ransomware attacks involving data theft, because warnings were readily available and accessible via the internet.

[10] Data breaches break record in 2021, CNET (Jan. 24, 2022), https://www.cnet.com/news/privacy/record-number-of-data-breaches-reported-in-2021-new-report-says/.

56. In April 2020, ZDNet reported, in an article titled "Ransomware mentioned in 1,000+ SEC filings over the past year," that "[r]ansomware gangs are now ferociously aggressive in their pursuit of big companies. They breach networks, use specialized tools to maximize damage, leak corporate information on dark web portals, and even tip journalists to generate negative news for companies as revenge against those who refuse to pay."[11]

57. In September 2020, the United States Cybersecurity and Infrastructure Security Agency published online a "Ransomware Guide" advising that "[m]alicious actors have adjusted their ransomware tactics over time to include pressuring victims for payment by threatening to release stolen data if they refuse to pay and publicly naming and shaming victims as secondary forms of extortion."[12]

58. This readily available and accessible information confirms that, prior to the Data Breach, Defendant knew or should have known that (i) ransomware actors were targeting entities such as Defendant, (ii) ransomware gangs were ferociously aggressive in their pursuit of entities such as Defendant, (iii) ransomware gangs were leaking corporate information on dark web portals, and (iv) ransomware tactics included threatening to release stolen data.

59. In light of the information readily available and accessible on the internet before the Data Breach, Defendant, having elected to store the unencrypted PII of its current and former employees in an Internet-accessible environment, had reason to be on guard for the exfiltration of the PII and Defendant's type of business had cause to be particularly on guard against such an attack.

---

[11] Ransomware mentioned in 1,000+ SEC filings over the past year, ZDNet, https://www.zdnet.com/article/ransomware-mentioned-in-1000-sec-filings-over-the-past-year/ (last accessed April 9, 2026).

[12] Ransomware Guide, U.S. CISA, https://www.cisa.gov/stopransomware/ransomware-guide (last accessed April 9, 2026).

60. Before the Data Breach, Defendant knew or should have known that there was a foreseeable risk that Plaintiffs' and Class Members' PII could be accessed, exfiltrated, and published as the result of a cyberattack. Notably, data breaches are prevalent in today's society therefore making the risk of experiencing a data breach entirely foreseeable to Defendant.

61. Prior to the Data Breach, Defendant knew or should have known that it should have encrypted its employees' Social Security numbers and other sensitive data elements within the PII to protect against their publication and misuse in the event of a cyberattack.

62. 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.

E. Defendant Failed to Follow FTC Guidelines

63. 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.

64. 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.[13] 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;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

[13] *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.

e. implement policies to correct security problems.

65. 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.

66. 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.

67. 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.

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

F. Defendant Fails to Comply with HIPAA and HITECH Requirements

69. Defendant is a covered business under HIPAA, 45 C.F.R. § 160.102, and is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164,

Subparts A and E, as well as the Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and C.

70. Defendant is also subject to the rules and regulations for safeguarding electronic forms of medical information pursuant to the Health Information Technology Act ("HITECH"). [14] *See* 42 U.S.C. § 17921; 45 C.F.R. § 160.103.

71. HIPAA's Privacy Rule or Standards for Privacy of Individually Identifiable Health Information establishes national standards for the protection of health information.

72. HIPAA's Privacy Rule or Security Standards for the Protection of Electronic Protected Health Information establishes a national set of security standards for protecting health information that is kept or transferred in electronic form.

73. HIPAA requires "compl[iance] with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302.

74. "Electronic protected health information" is "individually identifiable health information . . . that is (i) transmitted by electronic media; maintained in electronic media." 45 C.F.R. § 160.103.

75. HIPAA's Security Rule requires Defendant to do the following:

a. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits;

[14] HIPAA and HITECH work in tandem to provide guidelines and rules for maintaining protected health information. HITECH references and incorporates HIPAA.

b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and

d. Ensure compliance by its workforce.

76. HIPAA also requires Defendant to "review and modify the security measures implemented . . . as needed to continue provision of reasonable and appropriate protection of electronic protected health information." 45 C.F.R. § 164.306(e). Additionally, Defendant is required under HIPAA to "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1).

77. HIPAA and HITECH also obligate Defendant to implement policies and procedures to prevent, detect, contain, and correct security violations, and to protect against uses or disclosures of electronic PHI that are reasonably anticipated but not permitted by the privacy rules. *See* 45 C.F.R. § 164.306(a)(1) and § 164.306(a)(3); *see also* 42 U.S.C. § 17902.

78. HIPAA requires a covered entity to have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of 45 C.F.R. Part 164, Subparts D or E. *See* 45 C.F.R. § 164.530(e).

79. HIPAA requires a covered entity to mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of PHI in violation of its policies

and procedures or the requirements of 45 C.F.R. Part 164, Subpart E by the covered entity or its business associate. *See* 45 C.F.R. § 164.530(f).

80. HIPAA also requires the Office of Civil Rights ("OCR"), within the Department of Health and Human Services ("HHS"), to issue annual guidance documents on the provisions in the HIPAA Security Rule. *See* 45 C.F.R. §§ 164.302-164.318. For example, "HHS has developed guidance and tools to assist HIPAA covered entities in identifying and implementing the most cost effective and appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of e-PHI and comply with the risk analysis requirements of the Security Rule." U.S. Department of Health & Human Services, Security Rule Guidance Material.[15] The list of resources includes a link to guidelines set by the National Institute of Standards and Technology ("NIST"), which OCR says "represent the industry standard for good business practices with respect to standards for securing e-PHI." U.S. Department of Health & Human Services, Guidance on Risk Analysis.[16]

G. Defendant Failed to Follow Industry Standards

81. 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.

[15] https://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html (last accessed April 9, 2026).
[16] https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-riskanalysis/index.html (last accessed April 9, 2026).

82. 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.

83. Upon information and belief, Defendant failed to implement industry-standard cybersecurity measures, including failing to meet the minimum standards of 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).

84. 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.

H. Plaintiffs' Experiences and Injuries

Plaintiff Pamela Futrell-Parham

85. Plaintiff was an employee of Defendant.

86. Plaintiff Futrell-Parham was an employee of IRC at all times relevant hereto.

87. In connection with her employment, Plaintiff Futrell-Parham entrusted Defendant with her Private Information.

88. Plaintiff Futrell-Parham received a Notice of Data Breach Letter dated February 14, 2025, a true and correct copy of which is attached hereto as Exhibit A.

89. The Notice Letter stated that the files involved contained her name and Social Security number.

90. Plaintiff Futrell-Parham is especially alarmed both by the exposure of her Social Security number and by the vague nature of Defendant's notice regarding the full scope of the information accessed.

91. Since the Data Breach, Plaintiff Futrell-Parham has spent additional time monitoring her financial accounts, including approximately one hour per week, to guard against fraud and identity theft.

92. Since the Data Breach, Plaintiff Futrell-Parham began receiving an excessive number of spam calls on the same cell phone number she had provided to IRC.

93. Plaintiff Futrell-Parham also began receiving increased spam emails and text messages that were not typical before the Data Breach.

94. Plaintiff Futrell-Parham also received a fraud alert from the Internal Revenue Service and was required to obtain an additional security PIN for identity confirmation.

95. As a result of the Data Breach, Plaintiff Futrell-Parham has suffered lost time, anxiety, annoyance, distraction, and continuing concern over misuse of her Private Information.

96. Had Plaintiff Futrell-Parham known that Defendant would not adequately protect her Private Information, she would not have entrusted Defendant with it.

Plaintiff Steevenson Jolicoeur

97. Plaintiff Steevenson Jolicoeur is and at all times mentioned herein was an individual citizen of the State of Florida.

98. Plaintiff Jolicoeur received healthcare services from Defendant.

99. As a condition of receiving those services, Plaintiff Jolicoeur was required to provide Defendant with his Private Information, including PII and PHI.

100. At the time of the Data Breach, Defendant retained Plaintiff Jolicoeur's Private Information in its systems.

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

102. Plaintiff Jolicoeur learned of the Data Breach after receiving Defendant's Notice Letter.

103. According to the Notice Letter, Plaintiff Jolicoeur's Private Information was improperly accessed by unauthorized third parties.

104. The compromised information included at least his name and Social Security number.

105. As a result of the Data Breach, Plaintiff Jolicoeur made reasonable efforts to mitigate its effects, including checking his bills and accounts to make sure they were correct.

106. Plaintiff Jolicoeur has spent significant time dealing with the Data Breach, time he otherwise would have devoted to work, personal matters, and recreation, and that time cannot be recaptured.

107. As a result of the Data Breach, Plaintiff Jolicoeur fears for his personal financial security and remains uncertain about what information was revealed in the Data Breach.

108. Plaintiff Jolicoeur has suffered anxiety, sleep disruption, stress, and fear because of the Data Breach and the resulting invasion of privacy caused by the exposure of his private medical information.

109. Plaintiff Jolicoeur anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

110. Plaintiff Jolicoeur is presently at risk and will continue to face an increased risk of identity theft and fraud for years to come.

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

Plaintiff Jhovanna Salazar

112. Plaintiff Jhovanna Salazar is and at all times mentioned herein was an individual citizen of the State of California.

113. In exchange for employment, Plaintiff Salazar entrusted her Personal Information to Defendant. IRC was required to protect and maintain the confidentiality of the Personal Information entrusted to it by Plaintiff Salazar.

114. Plaintiff Salazar received a notice letter from Defendant dated February 14, 2025, informing her that her Personal Information, including her Social Security number, was specifically identified as having been exposed in the Data Breach.

115. Plaintiff Salazar is careful with her Personal Information.

116. Plaintiff Salazar entrusted her Personal Information to Defendant with the reasonable expectation and mutual understanding that Defendant would keep it confidential and secure from unauthorized access.

117. Because of the Data Breach, Plaintiff Salazar's Personal Information is now in the hands of cybercriminals, placing her at imminent risk of identity theft and fraud.

118. As a result of the Data Breach, Plaintiff Salazar has already expended time and suffered loss of productivity in addressing and attempting to mitigate the future consequences of the Data Breach, including investigating the breach, researching how best to protect herself from identity theft, reviewing account statements and other information, and taking other steps to mitigate the harm caused by the Data Breach.

119. Plaintiff Salazar is experiencing significant stress and anxiety as a result of learning that her Personal Information is in the hands of unauthorized cybercriminals.

120. Plaintiff Salazar has suffered injury directly and proximately caused by the Data Breach, including theft of her valuable Personal Information, the imminent and certainly impending injury flowing from fraud and identity theft, diminution in value of her Personal Information, and loss of the benefit of the bargain with Defendant to provide adequate and reasonable data security.

121. Plaintiff Salazar's Personal Information remains in Defendant's possession and remains at risk of further breaches so long as Defendant fails to undertake appropriate and adequate protective measures.

Plaintiff Jane Doe

122. Plaintiff Jane Doe is and at all times mentioned herein was an individual citizen of the State of Indiana residing in Hammond, Indiana.

123. Plaintiff Jane Doe is an employee of Defendant.

124. As a condition of her employment with Defendant, Plaintiff Jane Doe provided Defendant with her PII, which Defendant used to facilitate her employment, including payroll and

required Plaintiff to provide that PII in order to obtain employment and payment for that employment.

125. Plaintiff Jane Doe provided her PII to Defendant and trusted that Defendant would use reasonable measures to protect it according to its internal policies and applicable law.

126. Defendant obtained and continues to maintain Plaintiff Jane Doe's PII and has a continuing duty to protect that information from unauthorized access and disclosure.

127. Plaintiff Jane Doe reasonably understood that a portion of the funds derived from her employment would be used to pay for adequate cybersecurity and protection of PII.

128. Plaintiff Jane Doe received a Notice of Data Breach in February 2025.

129. Through the Data Breach, Defendant compromised at least Plaintiff Jane Doe's name and Social Security number.

130. Upon information and belief, Plaintiff Jane Doe's PII has already been published, or will be published imminently, by cybercriminals on the Dark Web.

131. Plaintiff Jane Doe has spent and will continue to spend significant time and effort monitoring her accounts to protect herself from identity theft.

132. In the aftermath of the Data Breach, Plaintiff Jane Doe suffered a spike in spam and scam phone calls and text messages.

133. On information and belief, Plaintiff Jane Doe's phone number was compromised as a result of the Data Breach.

134. Plaintiff Jane Doe fears for her personal financial security and worries about what information was exposed in the Data Breach.

135. Plaintiff Jane Doe has suffered and will continue to suffer anxiety, sleep disruption, stress, fear, and frustration as a result of the Data Breach.

136. Plaintiff Jane Doe suffered actual injury from the exposure and theft of her PII, including invasion of privacy and damages to and diminution in the value of her PII.

137. Plaintiff Jane Doe also faces imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft.

138. Plaintiff Jane Doe has spent—and will continue to spend – significant time and effort monitoring her accounts to protect herself from identity theft. After all, Defendant directed Plaintiff to take those steps in its breach notice.

139. Plaintiff Jane Doe has a continuing interest in ensuring that her PII, which upon information and belief remains backed up in Defendant's possession, is protected and safeguarded from additional breaches.

Plaintiff John Doe

140. Plaintiff John Doe is and at all times mentioned herein was an individual citizen of the State of Indiana residing in Whiting, Indiana.

141. Plaintiff John Doe is a current employee of Defendant.

142. As a condition of his employment with Defendant, Plaintiff John Doe provided Defendant with his PII, which Defendant used to facilitate his employment, including payroll.

143. Plaintiff John Doe provided his PII to Defendant and trusted that Defendant would use reasonable measures to protect it according to its internal policies and applicable law.

144. Defendant obtained and continues to maintain Plaintiff John Doe's PII and has a continuing duty to protect that information from unauthorized access and disclosure.

145. Plaintiff John Doe reasonably understood that a portion of the funds derived from his employment would be used to pay for adequate cybersecurity and protection of PII.

146. Plaintiff John Doe received a Notice of Data Breach in February 2025.

147. Through the Data Breach, Defendant compromised at least Plaintiff John Doe's name and Social Security number.

148. Upon information and belief, Plaintiff John Doe's PII has already been published, or will be published imminently, by cybercriminals on the Dark Web.

149. In the aftermath of the Data Breach, Plaintiff John Doe was notified that his information was found on the Dark Web.

150. Plaintiff John Doe has spent and will continue to spend significant time and effort monitoring his accounts to protect himself from identity theft.

151. Following the Data Breach, Plaintiff John Doe suffered a spike in spam and scam phone calls.

152. On information and belief, Plaintiff John Doe's phone number was compromised as a result of the Data Breach.

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

154. Plaintiff John Doe has suffered and will continue to suffer anxiety, sleep disruption, stress, fear, and frustration as a result of the Data Breach.

155. Plaintiff John Doe suffered actual injury from the exposure and theft of his PII, including invasion of privacy and damages to and diminution in the value of his PII.

156. Plaintiff John Doe also faces imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft.

157. Plaintiff John Doe anticipates spending considerable amounts of time and money to try to mitigate his injuries.

158. Plaintiff John Doe 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.

I. Plaintiffs and the Class Suffered Common Injuries and Damages Due to Defendant's Conduct

159. Because of Defendant's failure to prevent the Data Breach, Plaintiffs 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 recover 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 identity 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 at risk for future breaches so long as Defendant fails to take appropriate measures to protect the PII.

160. 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.

161. The value of Plaintiffs' 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.

162. 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.

163. 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.).

164. The development of "Fullz" packages means that the PII exposed in the Data Breach can easily be linked to data of Plaintiffs and the Class that is available on the internet.

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

166. Defendant disclosed the PII of Plaintiffs and Class members for criminals to use in the conduct of criminal activity. Specifically, Defendant opened up, disclosed, and exposed the PII of Plaintiffs 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.

167. Defendant's failure to promptly and properly notify Plaintiffs and Class members of the Data Breach exacerbated Plaintiffs' 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.

V. CLASS ACTION ALLEGATIONS

168. Plaintiffs bring 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 Innovative Renal Care in February 2024, including all those individuals who received notice of the breach.

169. 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.

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

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

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

173. 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 501 members.

174. Typicality. Plaintiffs' 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.

175. Adequacy. Plaintiffs will fairly and adequately protect the proposed Class's common interests. Their interests do not conflict with Class members' interests. And Plaintiffs have 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.

176. Commonality and Predominance. Plaintiffs' 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 Plaintiffs' 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 were negligent in maintaining, protecting, and securing PII;

d. if Defendant breached contract promises to safeguard Plaintiffs' 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 Plaintiffs and the Class injuries;

h. what the proper damages measure is; and

i. if Plaintiffs and the Class are entitled to damages, treble damages, and or injunctive relief.

177. 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 Plaintiffs and the Class)

178. Plaintiffs hereby repeat and reallege the preceding paragraphs of this Complaint and incorporate them by reference herein.

179. Plaintiffs 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.

180. Defendant owed a duty of care to Plaintiffs 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.

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

182. Defendant owed these duties to Plaintiffs 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 Plaintiffs and Class members' PII.

183. Defendant owed—to Plaintiffs 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 access;

c. promptly detect attempts at unauthorized access;

d. notify Plaintiffs and Class members within a reasonable timeframe of any breach to the security of their PII.

184. Thus, Defendant owed a duty to timely and accurately disclose to Plaintiffs and Class members the scope, nature, and occurrence of the Data Breach. After all, this duty is required and necessary for Plaintiffs 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.

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

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

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

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

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

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

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

192. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiffs' 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.

193. 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 Plaintiffs and Class members which actually and proximately caused the Data Breach and Plaintiffs' and Class members' injury.

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

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

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

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

198. Defendant's breach of its common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiffs 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 Plaintiffs and the Class)

199. Plaintiffs hereby repeat and reallege the preceding paragraphs of this Complaint and incorporate them by reference herein.

200. Pursuant to the Federal Trade Commission Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information.

201. Pursuant to HIPAA, 42 U.S.C. § 1320d et seq., Defendant had a duty to implement reasonable safeguards to protect Plaintiffs' and Class Members' Private Information.

202. Pursuant to HIPAA, Defendant also had a duty to render the electronic protected health information it maintained unusable, unreadable, or indecipherable to unauthorized individuals, as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key." *See* 45 C.F.R. § 164.304.

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

204. Defendant's failure to comply with applicable statutes, regulations, and legal duties constitutes negligence per se.

205. The injuries to Plaintiffs and Class Members resulting from the Data Breach were directly and indirectly caused by Defendant's violations of the statutes and regulations described herein.

206. Plaintiffs and Class Members are within the class of persons the FTC Act and HIPAA were intended to protect, and the type of harm that resulted from the Data Breach was the type of harm these authorities were intended to guard against.

207. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiffs and Class Members, Plaintiffs and Class Members would not have suffered the injuries alleged herein.

208. The injuries and harms suffered by Plaintiffs and Class Members were the reasonably foreseeable result of Defendant's breaches of duty. Defendant knew or should have known that its failure to meet these duties would cause Plaintiffs and Class Members to experience the foreseeable harms associated with the exposure of their Private Information.

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

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

210. Plaintiffs hereby repeat and reallege the preceding paragraphs of this Complaint and incorporate them by reference herein.

211. Plaintiffs incorporate by reference all other paragraphs as if fully set forth herein.

212. Plaintiffs and Class members were required to provide their PII to Defendant as a condition of receiving employment provided by Defendant. Plaintiffs and Class members provided their PII to Defendant or its third-party agents in exchange for Defendant's employment.

213. Plaintiffs and Class members reasonably understood that a portion of the funds derived from their employment would be used to pay for adequate cybersecurity measures.

214. Plaintiffs 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.

215. Plaintiffs and the Class members accepted Defendant's offers by disclosing their PII to Defendant or its third-party agents in exchange for employment.

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

217. In its Privacy Policy, Defendant represented that they had a legal duty to protect Plaintiffs' and Class Member's PII.

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

219. After all, Plaintiffs and Class members would not have entrusted their PII to Defendant in the absence of such an agreement with Defendant.

220. Plaintiffs and the Class fully performed their obligations under the implied contracts with Defendant.

221. 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.

222. 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.

223. Defendant materially breached the contracts it entered with Plaintiffs 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.

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

225. Defendant's material breaches were the direct and proximate cause of Plaintiffs' and Class members' injuries (as detailed *supra*).

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

227. Plaintiffs 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 Plaintiffs and the Class)

228. Plaintiffs hereby repeat and reallege the preceding paragraphs of this Complaint and incorporate them by reference herein.

229. Plaintiffs 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.

230. Defendant owed a duty to its current and former employees, including Plaintiffs and the Class, to keep this information confidential.

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

232. The intrusion was into a place or thing which was private and entitled to be private. Plaintiffs 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. Plaintiffs and the Class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

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

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

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

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

237. Indeed, Defendant's actions amount to intentional conduct because, given the ubiquity of data breaches on vulnerable companies, it must have known that a failure to implement reasonable cybersecurity measures would lead to a data breach. *See* Restatement (Second) of Torts § 8A.

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

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

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

241. Plaintiffs 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 Plaintiffs and the Class.

242. In addition to injunctive relief, Plaintiff, on behalf of herself 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 Plaintiffs and the Class)

243. Plaintiffs hereby repeat and reallege the preceding paragraphs of this Complaint and incorporate them by reference herein.

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

245. Plaintiffs and Class members conferred a benefit upon Defendant. After all, Defendant benefitted from using their employment and PII to derive profit and facilitate its business.

246. Defendant appreciated or had knowledge of the benefits it received from Plaintiffs and Class members.

247. Plaintiffs 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.

248. Defendant enriched itself by saving the costs they reasonably should have expended on data security measures to secure Plaintiffs' and Class members' PII.

249. 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 Plaintiffs and Class members by utilizing cheaper, ineffective security measures. Plaintiffs and Class members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

250. Under principles of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiffs' and Class members' employment and PII because Defendant failed to adequately protect their PII.

251. Plaintiffs and Class members have no adequate remedy at law.

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

SIXTH CAUSE OF ACTION
Violation of The California Consumer Privacy Act
Cal. Civ. Code §§ 1798.100, et seq.
(On Behalf of Plaintiff Salazar and the California Subclass)

253. Plaintiff Salazar ("Plaintiff," for purposes of this Cause) repeats, realleges, and incorporates by reference all preceding paragraphs as if fully set forth herein.

254. The California Consumer Privacy Act ("CCPA"), including Cal. Civ. Code § 1798.150(a), creates a private right of action for certain unauthorized access to and disclosure of covered personal information resulting from a business's failure to implement and maintain reasonable security procedures and practices.

255. Defendant is a "business" within the meaning of Cal. Civ. Code § 1798.140 because, upon information and belief, it is organized for profit or financial benefit and has annual gross revenues in excess of $25 million.

256. Plaintiff and California Subclass Members are "consumers" within the meaning of Cal. Civ. Code § 1798.140 because they are natural persons who are California residents.

257. The personal information at issue in this action constitutes "personal information" covered by Cal. Civ. Code §§ 1798.150(a) and 1798.81.5 because it includes an individual's first name or first initial and last name in combination with one or more unencrypted and unredacted data elements, including Social Security number, driver's license or identification number, tax identification number, financial account information, medical information, and health insurance information.

258. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard Plaintiff's and California Subclass Members' personal information and that the risk of unauthorized access, exfiltration, theft, or disclosure was reasonably foreseeable.

259. Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, and as a result Plaintiff's and California Subclass Members' nonencrypted and nonredacted personal information was subjected to unauthorized access, exfiltration, theft, or disclosure in the Data Breach.

260. As a direct and proximate result of Defendant's failure to maintain reasonable security procedures and practices, Plaintiff's and California Subclass Members' personal information was accessed, exfiltrated, stolen, or disclosed without authorization.

261. As a direct and proximate result of Defendant's conduct, Plaintiff and California Subclass Members suffered injury and lost money or property, including but not limited to loss of the confidentiality of their personal information, mitigation expenses, lost time, and other losses described herein.

262. Plaintiff and California Subclass Members also suffered stress, fear, and anxiety as a result of the Data Breach and the resulting loss of control over their personal information.

263. Cal. Civ. Code § 1798.150(b) provides that no prefiling notice is required before an individual consumer initiates an action solely for actual pecuniary damages.

264. On February 19, 2025, Plaintiff provided written notice to Defendant pursuant to Cal. Civ. Code § 1798.150(b) identifying the specific provisions of the CCPA alleged to have been violated and demanding that Defendant cure any curable violations within thirty (30) days. To the extent Defendant did not cure within the statutory 30-day period (and Plaintiff maintains that a cure is not possible), Plaintiff and the California Subclass are eligible to seek statutory damages as provided by Cal. Civ. Code § 1798.150(a).

265. Plaintiff and the California Subclass Members seek damages under the CCPA to the fullest extent possible. *See* Cal. Civ. Code § 1798.150.

SEVENTH CAUSE OF ACTION
Violation of the California Unfair Competition Law,
Cal. Bus. & Prof. Code § 17200 et seq
(On Behalf of Plaintiff Salazar and the California Subclass)

266. Plaintiff Salazar ("Plaintiff," for purposes of this Cause) repeats, realleges, and incorporates by reference the preceding paragraphs as if fully set forth herein.

267. Defendant is a "person" as defined by Cal. Bus. & Prof. Code § 17201.

268. Defendant violated Cal. Bus. & Prof. Code § 17200 et seq. ("UCL") by engaging in unlawful, unfair, and fraudulent business acts and practices.

269. Defendant's unfair acts and practices include failing to implement and maintain reasonable security measures to protect Plaintiff's and California Subclass Members' Personal Information from unauthorized access, disclosure, exfiltration, theft, and other misuse, which directly and proximately caused the Data Breach.

270. Defendant's unfair acts and practices further include failing to identify foreseeable security risks, remediate known security vulnerabilities, and adequately improve its security practices despite the well-known risk of cyberattacks targeting sensitive personal and medical information.

271. Defendant's conduct was contrary to legislatively declared public policy favoring the protection of consumers' personal information and requiring businesses entrusted with such information to use reasonable security measures, including the policies reflected in the FTC Act, 15 U.S.C. § 45, California's Customer Records Act, Cal. Civ. Code § 1798.80 et seq., and California's Consumer Privacy Act, including Cal. Civ. Code § 1798.150.

272. Defendant's conduct caused substantial injury to Plaintiff and California Subclass Members that was not outweighed by any countervailing benefits to consumers or competition and that Plaintiff and California Subclass Members could not reasonably have avoided because they had no reason to know Defendant's data security was inadequate.

273. Defendant also engaged in unlawful business acts and practices by violating California law, including Cal. Civ. Code § 1798.82, as well as the common law duties described herein.

274. Defendant's unlawful, unfair, and fraudulent acts and practices include failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and California Subclass Members' Personal Information.

275. Defendant's unlawful, unfair, and fraudulent acts and practices further include failing to identify foreseeable security and privacy risks and to remediate identified security and privacy vulnerabilities.

276. Defendant also failed to comply with duties pertaining to the security and privacy of Plaintiff's and California Subclass Members' Personal Information.

277. Defendant misrepresented that it would protect the privacy and confidentiality of Plaintiff's and California Subclass Members' Personal Information, including by implementing and maintaining reasonable security measures.

278. Defendant omitted, suppressed, and concealed the material fact that it did not reasonably or adequately secure Plaintiff's and California Subclass Members' Personal Information.

279. Defendant also omitted, suppressed, and concealed the material fact that it did not comply with its legal and common law duties to protect the security and privacy of Plaintiff's and California Subclass Members' Personal Information.

280. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers concerning the adequacy of Defendant's data security practices and its ability to protect the confidentiality of their Personal Information.

281. As a direct and proximate result of Defendant's unfair, unlawful, and fraudulent acts and practices, Plaintiff and California Subclass Members suffered injury in fact and lost money or property, including but not limited to time and expenses incurred monitoring their

financial accounts and credit, an increased and imminent risk of fraud and identity theft, and the loss of value of their Personal Information.

282. Plaintiff and California Subclass Members also suffered the loss of the benefit of their bargain, because they entrusted Defendant with their Personal Information with the understanding that Defendant would implement reasonable data security measures, but Defendant failed to do so.

283. By collecting, storing, and failing to adequately safeguard Plaintiff's and California Subclass Members' Personal Information, Defendant engaged in unfair, unlawful, and fraudulent conduct within the meaning of the UCL.

284. Defendant's conduct was intentional, knowing, unfair, and/or reckless.

285. Plaintiff and California Subclass Members seek all relief available under the UCL, including restitution, declaratory relief, injunctive relief, public injunctive relief, reasonable attorneys' fees and costs as permitted by law, and such other relief as the Court deems proper.

VI. PRAYER FOR RELIEF

Plaintiffs 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 Plaintiffs and the proposed Class, appointing Plaintiffs as class representatives, and appointing their counsel to represent the Class;

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

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

D. Awarding Plaintiffs and the Class damages, including applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;

E. Awarding restitution and damages to Plaintiffs and the Class in an amount to be determined at trial;

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

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

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

I. Granting other relief that this Court finds appropriate.

VII. DEMAND FOR JURY TRIAL

Plaintiffs demand a jury trial for all claims so triable.

Dated: April 10, 2026

/s/ J. Gerard Stranch IV

J. Gerard Stranch, IV (TN BPR 23045)
Grayson Wells, BPR (TN BPR 039658)
STRANCH, JENNINGS & GARVEY, PLLC
The Freedom Center
223 Rosa L. Parks Avenue, Suite 200
Nashville, TN 37203
Tel: (615) 254-8801
gstranch@stranchlaw.com
gwells@stranchlaw.com

Interim Lead Counsel

Danielle L. Perry*
Ra O. Amen*
Lisa A. White
MASON & PERRY LLP (Local Office)
9117 Millertown Pike
Mascot, TN 37806
Tel: (202) 429-2290
dperry@masonllp.com
ramen@masonllp.com
lwhite@masonllp.com

A. Brooke Murphy**
MURPHY LAW FIRM
4116 Wills Rogers Pkwy, Suite 700
Oklahoma City, OK 73108
Tel: (405) 389-4989
abm@murphylegalfirm.com

Raina Borrelli*
STRAUSS BORRELLI PLLC
980 N. Michigan Avenue, Suite 1610
Chicago, IL 60611
Tel: (872) 263-1100
raina@straussborrelli.com

Lynn A. Toops**
COHENMALAD, LLP
One Indiana Square, Suite 1400
Indianapolis, IN 46204
Tel: (317) 636-6481
ltoops@cohenmalad.com

David K. Lietz*
MILBERG, PLLC
5335 Wisconsin Ave., NW, Suite 440
Washington, DC 20015
Tel: (866) 252-0878
dlietz@milberg.com

Leanna A. Loginov*
SHAMIS & GENTILE, P.A.
14 NE First Avenue, Suite 705
Miami, FL 33132
Tel: (305) 479-2299
lloginov@shamisgentile.com

Pro hac vice
****Pro hac vice forthcoming***

Attorneys for Plaintiffs and the Proposed Class

CERTIFICATE OF SERVICE

I hereby certify that on this 10th day of April, 2026, the foregoing document was filed with the Clerk of the Court using the Court's CM/ECF filing system, which will serve notice on all counsel of record.

/s/ J. Gerard Stranch, IV
J. Gerard Stranch, (TN BPR 23045)