

**IN THE CIRCUIT COURT OF THE CITY OF ST. LOUIS
STATE OF MISSOURI**

TIFFANY RAYBURN and MARQUITA)	
PATTERSON, individually, and on behalf of all)	
others similarly situated,)	
)	
Plaintiffs,)	
)	Case No.:
v.)	
)	JURY TRIAL DEMANDED
MERS MISSOURI GOODWILL)	
INDUSTRIES,)	
)	
Defendant.)	
)	

CLASS ACTION PETITION

Plaintiffs Tiffany Rayburn and Marquita Patterson (“Plaintiffs”) bring this Class Action Petition (“Petition”) against Defendant MERS Missouri Goodwill Industries (“MERS” or “Defendant”) as individuals and on behalf of all others similarly situated, and allege, upon personal knowledge as to their own actions and their counsels’ investigation, and upon information and belief as to all other matters, as follows:

NATURE OF THE ACTION

1. This Class Action arises from a recent cyberattack resulting in a data breach of sensitive information in the possession and custody and/or control of Defendant (the “Data Breach”).
2. The Data Breach resulted in the unauthorized disclosure, exfiltration, and theft of current and former employees’ personally identifiable information and personal health information, including full names, dates of birth, Social Security numbers, and medical diagnosis information (collectively the “PII/PHI”).¹

¹ MERS Goodwill Notice of Data Security Incident, MERS Missouri Goodwill Industries, <https://mersgoodwill.org/notice-of-data-security-incident/> (last visited May 28, 2024).

3. On information and belief, the Data Breach occurred between March 10, 2023 and March 15, 2023. However, it is unclear when MERS became aware of the breach due to the obfuscating nature of its breach notice.

4. On May 9, 2024, over a year and two months after the breach occurred, MERS finally notified Plaintiffs and Class Members about the widespread Data Breach (“Notice Letter”). Plaintiff Patterson’s Notice Letter is attached as **Exhibit A**. A standard Notice Letter is attached as **Exhibit B**.

5. MERS waited over fourteen months after the Data Breach began before informing Class Members, even though Plaintiffs and Class Members had their most sensitive personal information accessed, exfiltrated, and stolen, causing them to suffer ascertainable losses in the form of the loss of the benefit of their bargain and the value of their time reasonably incurred to remedy or mitigate the effects of the attack.

6. MERS’ Breach Notice obfuscated the nature of the breach and the threat it posed—refusing to tell victims how many people were impacted, how the breach happened on MERS’ systems, when MERS discovered the Data Breach, or why it took MERS fourteen months to begin notifying victims that hackers had gained access to highly sensitive PII/PHI.

7. Defendant’s failure to timely detect and report the Data Breach made its current and former employees vulnerable to identity theft without any warnings to monitor their financial accounts or credit reports to prevent unauthorized use of their PII/PHI.

8. Defendant knew or should have known that each victim of the Data Breach deserved prompt and efficient notice of the Data Breach and assistance in mitigating the effects of PII/PHI misuse.

9. In failing to adequately protect Plaintiffs' and the Class's PII/PHI, failing to adequately notify them about the breach, and by obfuscating the nature of the breach, Defendant violated state and federal law and harmed an unknown number of its current and former employees.

10. Plaintiffs and members of the proposed Class are victims of Defendant's negligence and inadequate cyber security measures. Specifically, Plaintiffs and members of the proposed Class trusted Defendant with their PII/PHI. But Defendant betrayed that trust. Defendant failed to properly use up-to-date security practices to prevent the Data Breach.

11. Plaintiffs are Data Breach victims.

12. Accordingly, Plaintiffs, on their own behalf and on behalf of a class of similarly situated individuals, bring this lawsuit seeking injunctive relief, damages, and restitution, together with costs and reasonable attorneys' fees, the calculation of which will be based on information in Defendant's possession.

PARTIES

13. Plaintiff, Marquita Patterson, is a natural person and citizen of Missouri, where she intends to remain.

14. Plaintiff, Tiffany Rayburn, is a natural person and citizen of Missouri, where she intends to remain.

15. Defendant, MERS, is a Missouri non-profit organization with its principal place of business at 1727 Locust Street, St. Louis, MO 63103.

JURISDICTION AND VENUE

16. This Court has personal jurisdiction over Defendant because it regularly conducts business throughout Missouri and has its principal place of business at 1727 Locust St, St. Louis, MO 63103.

17. Venue is appropriate in this Court because Plaintiffs were first injured by Defendant's conduct that occurred in the city of St. Louis. Mo. Rev. Stat. § 508.010.

STATEMENT OF FACTS

MERS

18. MERS is a non-profit organization that offers programs and services including career counseling, skills training, education and literacy programs, employment services, and more.² MERS boasts a total annual revenue of \$224 million.³

19. As an organization that annually serves more than 11,000 individuals and operates over 42 career centers,⁴ MERS understood the need to protect its own employees' data, as well as prioritize its data security.

20. Indeed, MERS promises in its privacy policy that it "recognizes the importance of protecting information we may collect." Defendant also states that in order to "prevent unauthorized access, maintain data accuracy, and to ensure the appropriate use of information, we have put in place appropriate physical, electronic, and managerial procedures to safeguard and secure the information we collect."⁵

21. Despite recognizing its duty to do so, on information and belief, MERS has not implemented reasonably cybersecurity safeguards or policies to protect its current and former

² About, MERS Goodwill, <https://mersgoodwill.org/about/> (last visited May 28, 2024).

³ MERS Goodwill, ProPublica, <https://projects.propublica.org/nonprofits/organizations/430652657> (last visited May 28, 2024).

⁴ Home, MERS Goodwill, <https://mersgoodwill.org/> (last visited May 28, 2024).

⁵ Privacy Policy, MERS Goodwill, <https://mersgoodwill.org/privacy-policy/> (last visited May 28, 2024).

employees' PII/PHI or supervised its IT or data security agents and employees to prevent, detect, and stop breaches of its systems. As a result, MERS leaves significant vulnerabilities in its systems for cybercriminals to exploit and gain access to current and former employees' PII/PHI.

The Data Breach

22. As a condition of employment with MERS, Defendant requires its employees, including Plaintiffs, to disclose PII including but not limited to, their names, dates of birth, and Social Security numbers. Defendant used that PII to facilitate its employment of Plaintiffs, including payroll, and required Plaintiffs to provide that PII to apply for employment and payment for that employment.

23. On information and belief, Defendant collects and maintains current and former employees' PII/PHI in its computer systems.

24. In collecting and maintaining PII/PHI, Defendant implicitly agrees that it will safeguard the data using reasonable means according to its internal policies, as well as state and federal law.

25. According to the Breach Notice, on or about March 10, 2023, "an unauthorized party accessed and removed a limited number of files from [MERS'] computer systems." An internal investigation revealed that the files were not only accessed but also "removed by the unauthorized party." Ex. A

26. In other words, MERS' investigation revealed that its network had been hacked by cybercriminals an appalling fourteen months before notice was sent to victims and that Defendant's cyber and data security systems were completely inadequate and allowed cybercriminals to obtain files containing a treasure trove of current and former employees' highly private PII/PHI.

27. Most data breach notice letters will, at minimum, admit to the date of the breach as well as when the breach was discovered. Not Defendant. Instead, Defendant intentionally obfuscates the appallingly long period between the date of the Breach and when Defendant discovered it, leaving Plaintiffs and Class Members in the dark.

28. Through its inadequate security practices, Defendant exposed Plaintiffs' and the Class's PII/PHI for theft and sale on the dark web.

29. On or around May 9, 2024—an astonishing one year and two months after the Breach first occurred – MERS finally notified Plaintiffs and Class Members about the Data Breach.

30. Despite its duties and alleged commitments to safeguard PII/PHI, Defendant did not in fact follow industry standard practices in securing current and former employees' PII/PHI, as evidenced by the Data Breach.

31. In response to the Data Breach, Defendant contends that it “continue[s] to take significant measures to protect your information.” Ex. A. Although Defendant fails to expand on what these alleged “measures” are, such steps should have been in place before the Data Breach.

32. Through its Breach Notice, Defendant also recognized the actual imminent harm and injury that flowed from the Data Breach, so it recommended “placing a Fraud Alert and Security Freeze on your credit files and obtaining a free credit report” and encouraged breach victims to “remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis.” Ex. B.

33. Through the Data Breach, Defendant recognized its duty to implement reasonable cybersecurity safeguards or policies to protect current and former employees PII/PHI, insisting that, despite the Data Breach demonstrating otherwise, Defendant is “committed to maintaining

the privacy of personal information in our possession and have taken many precautions to safeguard it.” Ex. B.

34. Cybercriminals need not harvest a person’s Social Security number or financial account information in order to commit identity fraud or misuse Plaintiffs' and the Class’s PII/PHI. Cybercriminals can cross-reference the data stolen from the Data Breach and combine with other sources to create “Fullz” packages, which can then be used to commit fraudulent account activity on Plaintiffs' and the Class’s financial accounts.

35. On information and belief, MERS has offered several months of complimentary credit monitoring services to victims, which does not adequately address the lifelong harm that victims will face following the Data Breach. Indeed, the breach involves PII/PHI that cannot be changed, such as Social Security numbers.

36. Even with several months of credit monitoring services, the risk of identity theft and unauthorized use of Plaintiffs' and Class Members’ PII/PHI is still substantially high. The fraudulent activity resulting from the Data Breach may not come to light for years.

37. Because of the Data Breach, Defendant inflicted injuries upon Plaintiffs and Class Members. And yet, Defendant has done absolutely nothing to provide Plaintiffs and the Class Members with relief for the damages they suffered and will suffer.

38. On information and belief, Defendant failed to adequately train and supervise its IT and data security agents and employees on reasonable cybersecurity protocols or implement reasonable security measures, causing it to lose control over its employees’ PII/PHI. Defendant’s negligence is evidenced by its failure to prevent the Data Breach and stop cybercriminals from accessing the PII/PHI.

Royal claims credit—and publishes the stolen PII/PHI

39. Worryingly, the cybercriminals that obtained Plaintiff’s and Class members’ PII/PHI appear to be the notorious cybercriminal group “Royal” ransomware group.⁶

40. On March 27, 2023, Royal ransomware group claimed credit for the Data Breach on its Dark Web website.⁷

41. Thereafter, Royal ransomware indicated it would *publish* the stolen PII/PHI, stating “we are ready to share some info with you” and providing a link to the files.



42. Thus, it appears Plaintiffs’ and Class members’ PII/PHI was already published on the Dark Web.

43. Royal ransomware group emerged in early 2022 and is suspected to consist of former members of other ransomware groups. It is reported to be the “most prolific ransomware in the e-crime landscape, overtaking Lockbit for the first time in more than a year.”⁸

⁶ This Week in Ransomware: May 17, 2024, Comparitech, <https://www.comparitech.com/news/the-week-in-ransomware-may-17-2024/> (last visited May 29, 2024).

⁷ FalconFeeds, Twitter, <https://x.com/FalconFeedsio/status/1641032465388011523> (last visited May 29, 2024).

⁸ Royal Rumble: Analysis of Royal Ransomware, Cybereason, <https://www.cybereason.com/blog/royal-ransomware-analysis> (last visited May 29, 2024).

44. Thus, the Cybersecurity and Infrastructure Security Agency (CISA) and FBI have warned that Royal:

- a. “uses its own custom-made file encryption program”;
- b. does “not include ransom amounts and payment instructions as part of the initial ransom note. Instead, the note, which appears after encryption, requires victims to directly interact with the threat actor”; and
- c. “has targeted over 350 known victims worldwide and ransomware demands have exceeded 275 million USD.”⁹

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

The Data Breach was a Foreseeable Risk of which Defendant was on Notice.

46. Defendant’s data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in the industry preceding the date of the breach.

47. In light of recent high profile data breaches at other companies in its industry, Defendant knew or should have known that its electronic records and current and former employees’ PII/PHI would be targeted by cybercriminals.

48. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.¹⁰ The 330 reported

⁹ #StopRansomware: Royal Ransomware, CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY, <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-061a>

¹⁰ 2021 Data Breach Annual Report, ITRC, [chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.wsav.com/wp-content/uploads/sites/75/2022/01/20220124_ITRC-2021-Data-Breach-Report.pdf](https://www.wsav.com/wp-content/uploads/sites/75/2022/01/20220124_ITRC-2021-Data-Breach-Report.pdf) (last visited June 5, 2023).

breaches reported in 2021 exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.¹¹

49. Indeed, cyberattacks have become increasingly common for over ten years, with the FBI warning as early as 2011 that cybercriminals were “advancing their abilities to attack a system remotely” and “[o]nce a system is compromised, cyber criminals will use their accesses to obtain PII.” The FBI further warned that that “the increasing sophistication of cyber criminals will no doubt lead to an escalation in cybercrime.”¹²

50. Cyberattacks on companies like Defendant 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 prepared for, a potential attack. As one report explained, “[e]ntities like smaller municipalities and hospitals are attractive. . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly.”¹³

51. 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 MERS.

Plaintiff Patterson’s Experience

52. Plaintiff Patterson is a former employee of MERS.

53. Plaintiff Patterson received MERS’ Breach Notice in or around May 2024.

54. Defendant deprived Plaintiff of the earliest opportunity to guard herself against the Data Breach’s effects by failing to notify her about it for fourteen months.

¹¹ *Id.*

¹² Gordon M. Snow Statement, FBI <https://archives.fbi.gov/archives/news/testimony/cyber-security-threats-to-the-financial-sector> (last visited March 13, 2023).

¹³ Secret Service Warn of Targeted, Law360, <https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware> (last visited March 13, 2023).

55. As a result of its inadequate cybersecurity, Defendant exposed Plaintiff for theft by cybercriminals and sale on the dark web.

56. Upon information and belief, through its Data Breach, Defendant compromised at least Plaintiff's full name, date of birth, and Social Security number.

57. As a result of the Data Breach notice, Plaintiff spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach, self-monitoring her accounts and credit reports to ensure no fraudulent activity has occurred. This time has been lost forever and cannot be recaptured.

58. Plaintiff has and will spend considerable time and effort monitoring her accounts to protect herself from additional identity theft. Plaintiff fears for her personal financial security and uncertainty over what PII/PHI was exposed in the Data Breach.

59. Plaintiff has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

60. Plaintiff suffered actual injury in the form of damages to and diminution in the value of Plaintiff's PII/PHI—a form of intangible property that Plaintiff entrusted to Defendant, which was compromised in and as a result of the Data Breach.

61. Plaintiff suffered actual injury from the exposure and theft of her PII/PHI—which violates her rights to privacy.

62. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PII/PHI being placed in the hands of unauthorized third parties and possibly criminals.

63. Indeed, following the Data Breach, Plaintiff's bank card was fraudulently used to make unauthorized purchases. These fraudulent transactions suggest that her PII, including her bank account information, which was provided to Defendant during her employment, has been stolen as a result of the Data Breach and is now in the hands of cybercriminals.

64. Further, following the Data Breach, Plaintiff has experienced a dramatic increase in spam calls and emails, suggesting that her PII/PHI is now in the hands of cybercriminals.

65. Once an individual's PII/PHI is for sale and access on the dark web, as Plaintiff's PII/PHI is here as a result of the Breach, cybercriminals are able to use the stolen and compromised to gather and steal even more information.¹⁴ On information and belief, Plaintiff's phone number was compromised as a result of the Data Breach.

66. Plaintiff has a continuing interest in ensuring that her PII/PHI, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches.

Plaintiff Rayburn's Experience

67. Plaintiff Rayburn is a former employee of MERS'.

68. Plaintiff received MERS' Breach Notice on or around May 2024.

69. Defendant deprived Plaintiff of the earliest opportunity to guard herself against the Data Breach's effects by failing to notify her about it for fourteen months.

70. As a result of its inadequate cybersecurity, Defendant exposed Plaintiff's PII/PHI for theft by cybercriminals and sale on the dark web.

¹⁴ What do Hackers do with Stolen Information, Aura, <https://www.aura.com/learn/what-do-hackers-do-with-stolen-information> (last visited January 9, 2024).

71. Upon information and belief, through its Data Breach, Defendant compromised at least Plaintiff's full name, date of birth, and Social Security number.

72. As a result of the Data Breach notice, Plaintiff spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach, contacting credit bureaus, and self-monitoring her accounts and credit reports to ensure no fraudulent activity has occurred. This time has been lost forever and cannot be recaptured.

73. Plaintiff has and will spend considerable time and effort monitoring her accounts to protect herself from additional identity theft. Plaintiff fears for her personal financial security and uncertainty over what PII/PHI was exposed in the Data Breach.

74. Plaintiff has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

75. Plaintiff suffered actual injury in the form of damages to and diminution in the value of Plaintiff's PII/PHI —a form of intangible property that Plaintiff entrusted to Defendant, which was compromised in and as a result of the Data Breach.

76. Plaintiff suffered actual injury from the exposure and theft of her PII/PHI—which violates her rights to privacy.

77. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PII/PHI being placed in the hands of unauthorized third parties and possibly criminals.

78. Indeed, following the Data Breach, Plaintiff spent time contacting credit bureaus to determine whether her credit was impacted by the Data Breach. She was informed by the credit bureau that there were multiple unauthorized hard inquiries on her credit report since 2023 that she did not recognize. The credit bureau also informed Plaintiff that a P.O. box address was being used in connection with her name and an unauthorized actor was using the name “Tiffany Smith” to commit acts of fraud using Plaintiff’s information.

79. Following the Data Breach, Plaintiff has experienced numerous instances of fraud in the form of an unauthorized actor fraudulently taking out loans, mortgages, and credit cards with Plaintiff’s information, including:

- a. In April 2023, an unauthorized actor fraudulently took out a mortgage in Plaintiff’s name;
- b. In April 2023, 10 credit cards were fraudulently taken out in Plaintiff’s name, including a credit card with Chase bank;
- c. In May 2023 an unauthorized actor fraudulently took out a loan in Plaintiff’s name in Las Vegas; and
- d. In February 2024, a car loan was fraudulently taken out in Plaintiff’s name.

80. Following the Data Breach, Plaintiff has also experienced an enormous increase in spam calls, emails, and mail, including calls trying to convince Plaintiff to make purchases, calls claiming to be insurance companies, and mail that claims that Plaintiff purchased a car. This suggests that her PII/PHI has been stolen and is now in the hands of cybercriminals.

81. Once an individual’s PII/PHI is for sale and access on the dark web, as Plaintiffs’ PII/PHI is here as a result of the Breach, cybercriminals are able to use the stolen

and compromised to gather and steal even more information.¹⁵ On information and belief, Plaintiff's phone number was compromised as a result of the Data Breach.

82. Plaintiff has a continuing interest in ensuring that her PII/PHI, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches.

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

83. Plaintiffs and members of the proposed Class have suffered injury from the misuse of their PII/PHI that can be directly traced to Defendant.

84. As a result of Defendant's failure to prevent the Data Breach, Plaintiffs and the proposed Class have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at an increased risk of suffering:

- a. The loss of the opportunity to control how their PII/PHI is used;
- b. The diminution in value of their PII/PHI;
- c. The compromise and continuing publication of their PII/PHI;
- d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;
- e. Lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent

¹⁵ What do Hackers do with Stolen Information, Aura, <https://www.aura.com/learn/what-do-hackers-do-with-stolen-information> (last visited January 9, 2024).

researching how to prevent, detect, contest, and recover from identity theft and fraud;

- f. Delay in receipt of tax refund monies;
- g. Unauthorized use of stolen PII/PHI; and
- h. The continued risk to their PII/PHI, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake the appropriate measures to protect the PII/PHI in its possession.

85. 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.

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

87. It can take victims years to spot identity theft, giving criminals plenty of time to use that information for cash.

88. One such example of criminals using PII/PHI for profit is the development of "Fullz" packages.

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

90. The development of “Fullz” packages means that stolen PII/PHI from the Data Breach can easily be used to link and identify it to Plaintiffs and the proposed Class’ phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII/PHI 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 members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiffs’ and the Class’s stolen PII/PHI is being misused, and that such misuse is fairly traceable to the Data Breach.

91. Defendant disclosed the PII/PHI of Plaintiffs and the Class for criminals to use in the conduct of criminal activity. Specifically, Defendant opened up, disclosed, and exposed the PII/PHI of Plaintiffs and the Class to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen PII/PHI.

92. Defendant’s failure to properly notify Plaintiffs and members of the Class of the Data Breach exacerbated Plaintiffs’ and the Class’s injury by depriving them of the earliest ability to take appropriate measures to protect their PII/PHI and take other necessary steps to mitigate the harm caused by the Data Breach.

Defendant failed to adhere to FTC guidelines.

93. According to the Federal Trade Commission (“FTC”), the need for data security should be factored into all business decision-making. To that end, the FTC has issued

numerous guidelines identifying best data security practices that businesses, such as Defendant, should employ to protect against the unlawful exposure of PII/PHI.

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

- a. protect the sensitive consumer information that it keeps;
- b. properly dispose of PII/PHI that is no longer needed;
- c. encrypt information stored on computer networks;
- d. understand their network's vulnerabilities; and
- e. implement policies to correct security problems.

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

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

97. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect consumer data, treating the failure to employ 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.

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

Defendant Fails to Comply with Industry Standards

99. As noted above, experts studying cyber security routinely identify entities in possession of PII/PHI as being particularly vulnerable to cyberattacks because of the value of the PII/PHI which they collect and maintain.

100. Several best practices have been identified that a minimum should be implemented by employers in possession of PII/PHI, like Defendant, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data and limiting which employees can access sensitive data. Defendant failed to follow these industry best practices, including a failure to implement multi-factor authentication.

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

102. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5,

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

103. These foregoing frameworks are existing and applicable industry standards for an employer's obligations to provide adequate data security for its employees. Upon information and belief, Defendant failed to comply with at least one—or all—of these accepted standards, thereby opening the door to the threat actor and causing the Data Breach.

Defendant Violated HIPAA

104. HIPAA circumscribes security provisions and data privacy responsibilities designed to keep patients' medical information safe. HIPAA compliance provisions, commonly known as the Administrative Simplification Rules, establish national standards for electronic transactions and code sets to maintain the privacy and security of protected health information.¹⁶

105. HIPAA provides specific privacy rules that require comprehensive administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of PII and PHI is properly maintained.¹⁷

106. The Data Breach itself resulted from a combination of inadequacies showing Defendant failed to comply with safeguards mandated by HIPAA. Defendant's security failures include, but are not limited to:

¹⁶ HIPAA lists 18 types of information that qualify as PHI according to guidance from the Department of Health and Human Services Office for Civil Rights, and includes, *inter alia*: names, addresses, any dates including dates of birth, Social Security numbers, and medical record numbers.

¹⁷ See 45 C.F.R. § 164.306 (security standards and general rules); 45 C.F.R. § 164.308 (administrative safeguards); 45 C.F.R. § 164.310 (physical safeguards); 45 C.F.R. § 164.312 (technical safeguards).

- a. Failing to ensure the confidentiality and integrity of electronic PHI that it creates, receives, maintains, and transmits in violation of 45 C.F.R. § 164.306(a)(1);
- b. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);
- c. Failing to protect against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);
- d. Failing to ensure compliance with HIPAA security standards by Defendant's workforce in violation of 45 C.F.R. § 164.306(a)(4);
- e. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);
- f. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. § 164.308(a)(1);
- g. Failing to identify and respond to suspected or known security incidents and failing to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. § 164.308(a)(6)(ii);
- h. Failing to effectively train all staff members on the policies and procedures

with respect to PHI as necessary and appropriate for staff members to carry out their functions and to maintain security of PHI in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5); and

- i. Failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PHI, in compliance with 45 C.F.R. § 164.530(c).

107. Simply put, the Data Breach resulted from a combination of insufficiencies that demonstrate Defendant failed to comply with safeguards mandated by HIPAA regulations.

CLASS ACTION ALLEGATIONS

108. Pursuant to Missouri Court Rule of Civil Procedure 52.08, Plaintiffs bring this class action on behalf of himself and the following proposed Class (the “Class”):

All individuals residing in the United States whose PII/PHI was compromised in the MERS Data Breach including all those who received notice of the breach.

109. Excluded from the Class is 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.

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

111. Plaintiffs and the Class Members satisfy the numerosity, commonality, typicality, adequacy, and predominance prerequisites for suing as representative parties pursuant to Rule 52.08(a).

- a. **Numerosity**. Plaintiffs’ claim is representative of the proposed Class, consisting of approximately 70,390 individuals, far too many to join in a single action;

- b. **Ascertainability**. Class members are readily identifiable from information

in Defendant's possession, custody, and control;

c. **Typicality**. Plaintiffs' claim is typical of Class member's 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.

d. **Adequacy**. Plaintiffs will fairly and adequately protect the proposed Class's interests. His interest does not conflict with Class members' interests, and Plaintiffs have retained counsel experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf, including as lead counsel.

e. **Commonality**. Plaintiffs and the Class's claims raise predominantly common fact and legal questions that a class wide proceeding can answer for all Class members. Indeed, it will be necessary to answer the following questions:

- i. Whether Defendant had a duty to use reasonable care in safeguarding Plaintiffs' and the Class's PII/PHI;
- ii. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
- iii. Whether Defendant was negligent in maintaining, protecting, and securing PII/PHI;
- iv. Whether Defendant breached contract promises to safeguard Plaintiffs and the Class's PII/PHI;
- v. Whether Defendant took reasonable measures to determine the extent of the Data Breach after discovering it;
- vi. Whether Defendant's Breach Notice was reasonable;

- vii. Whether the Data Breach caused Plaintiffs' and the Class's injuries;
- viii. What the proper damages measure is; and
- ix. Whether Plaintiffs and the Class are entitled to damages, treble damages, or injunctive relief.

f. **Appropriateness.** The likelihood that individual members of the Class will prosecute separate actions is remote due to the time and expense necessary to prosecute an individual case. Plaintiffs are not aware of any litigation concerning this controversy already commenced by others who meet the criteria for class membership described above.

g. Further, common questions of law and fact predominate over any individualized questions, and a class action is superior to individual litigation or any other available method to fairly and efficiently adjudicate the controversy. The damages available to individual plaintiffs are insufficient to make individual lawsuits economically feasible.

FIRST CLAIM FOR RELIEF
Negligence
(On Behalf of Plaintiffs and the Class)

112. Plaintiffs incorporate all previous paragraphs as if fully set forth herein.

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

114. 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/PHI in a data breach. And here, that foreseeable danger came to pass.

115. Defendant has full knowledge of the sensitivity of the PII/PHI and the types of harm

that Plaintiffs and the Class could and would suffer if their PII/PHI was wrongfully disclosed.

116. 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/PHI.

117. Defendant owed—to Plaintiffs and Class Members—at least the following duties to:

- a. exercise reasonable care in handling and using the PII/PHI in its care and custody;
- b. implement industry-standard security procedures sufficient to reasonably protect the information from a data breach, theft, and unauthorized;
- c. promptly detect attempts at unauthorized access;
- d. notify Plaintiffs and Class Members within a reasonable timeframe of any breach to the security of their PII/PHI.

118. Also, 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/PHI, 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.

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

120. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the PII/PHI 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.

121. 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/PHI, a necessary part of employment and/or obtaining manufacturing services from Defendant.

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

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

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

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

126. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiffs' and Class Members' PII/PHI by:

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

127. Defendant breached its duties by failing to exercise reasonable care in supervising its agents, contractors, vendors, and suppliers, and in handling and securing the PII/PHI of

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

128. 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.

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

130. 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.

131. 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/PHI by criminals, improper disclosure of their PII/PHI, lost benefit of their bargain, lost value of their PII/PHI, 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 CLAIM FOR RELIEF
Negligence *per se*
(On Behalf of Plaintiffs and the Class)

132. Plaintiffs incorporate all previous paragraphs as if fully set forth herein.

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

134. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce,"

including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect the PII/PHI entrusted to it. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiffs' and the Class Members' sensitive PII/PHI.

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

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

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

138. But for Defendant's wrongful and negligent breach of its duties owed, Plaintiffs and Class Members would not have been injured.

139. The injury and harm suffered by Plaintiffs and Class Members was the reasonably foreseeable result of Defendant's breach of their duties. Defendant knew or should have known that Defendant was failing to meet its duties and that its breach would cause Plaintiffs and members of the Class to suffer the foreseeable harms associated with the exposure of their PII/PHI.

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

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

THIRD CLAIM FOR RELIEF
Breach of Implied Contract
(On Behalf of Plaintiffs and the Class)

142. Plaintiffs incorporate all previous paragraphs as if fully set forth herein.

143. Defendant offered to employ or provide services to Plaintiffs and members of the Class if, as a condition of that employment or of receiving services, Plaintiffs and members of the Class provided Defendant with their PII/PHI.

144. In turn, Defendant agreed it would not disclose the PII/PHI it collects to unauthorized persons. Defendant also promised to safeguard employee or client PII/PHI.

145. Plaintiffs and the members of the Class accepted Defendant's offers by providing PII/PHI to Defendant in exchange for employment with Defendant.

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

147. Plaintiffs and the members of the Class would not have entrusted their PII/PHI to Defendant in the absence of such an agreement with Defendant.

148. Defendant materially breached the contracts it had entered with Plaintiffs and members of the Class by failing to safeguard such information and failing to notify them promptly of the intrusion into its computer systems that compromised such information. Defendant also breached the implied contracts with Plaintiffs and members of the Class by:

- a. Failing to properly safeguard and protect Plaintiffs' and members of the Class's

PII/PHI;

- b. Failing to comply with industry standards as well as legal obligations that are necessarily incorporated into the parties' agreement; and
- c. Failing to ensure the confidentiality and integrity of electronic PII/PHI that Defendant created, received, maintained, and transmitted.

149. The damages sustained by Plaintiffs and members of the Class as described above were the direct and proximate result of Defendant's material breaches of its agreement(s).

150. Plaintiffs and members of the Class have performed under the relevant agreements, or such performance was waived by the conduct of Defendant.

151. The covenant of good faith and fair dealing is an element of every contract. All such contracts impose upon each party a duty of good faith and fair dealing. The 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—not merely the letter—of the bargain. Put differently, the parties to a contract are mutually obligated to comply with the substance of their contract in addition to its form.

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

153. Defendant failed to advise Plaintiffs and members of the Class of the Data Breach promptly and sufficiently.

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

155. Plaintiffs and members of the Class have sustained damages because of Defendant's

breaches of its agreement, including breaches of it through violations of the covenant of good faith and fair dealing.

156. Plaintiffs, on behalf of themselves and the Class, seek compensatory damages for breach of implied contract, which includes the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest, and costs.

FOURTH CLAIM FOR RELIEF
Unjust Enrichment
(On Behalf of the Plaintiffs and the Class)

157. Plaintiffs incorporate all previous paragraphs as if fully set forth herein.

158. This claim is plead in the alternative to the breach of implied contractual duty claim.

159. Plaintiffs and members of the Class conferred a benefit upon Defendant in the form of services through employment. Defendant also benefited from the receipt of Plaintiffs' and the Class's PII/PHI, as this was used to facilitate their employment.

160. Defendant appreciated or had knowledge of the benefits conferred upon itself by Plaintiffs and members of the Class.

161. Under principals of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiffs' and the proposed Class's services and their PII/PHI because Defendant failed to adequately protect their PII/PHI. Plaintiffs and the proposed Class would not have provided their PII/PHI or worked for Defendant at the payrates they did had they known Defendant would not adequately protect their PII/PHI.

162. Defendant should be compelled to disgorge into a common fund to benefit Plaintiffs and members of the Class all unlawful or inequitable proceeds received by it as a result of the conduct and Data Breach alleged here.

FIFTH CLAIM FOR RELIEF
Breach of Fiduciary Duty
(On Behalf of Plaintiffs and the Class)

163. Plaintiffs reallege all previous paragraphs as if fully set forth below.

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

165. Defendant has a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of Defendant's relationship with them—especially to secure their PII/PHI.

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

167. Defendant breached its fiduciary duties to Plaintiffs and Class Members by failing to sufficiently encrypt or otherwise protect Plaintiffs' and Class Members' PII/PHI.

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

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

PRAYER FOR RELIEF

Plaintiffs and members of the Class demand a jury trial on all claims so triable and request that the Court enter an order:

- A. Certifying this case as a class action on behalf of Plaintiffs and the proposed Class, appointing Plaintiff as class representative, and appointing his counsel to represent the Class;
- B. Awarding declaratory and other equitable relief as is necessary to protect the interests of Plaintiff and the Class;
- C. Awarding injunctive relief as is necessary to protect the interests of Plaintiff and the Class;
- D. Enjoining Defendant from further deceptive practices and making untrue statements about the Data Breach and the stolen PII/PHI;
- E. Awarding Plaintiff and the Class damages that include applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;
- F. Awarding restitution and damages to Plaintiff and the Class in an amount to be determined at trial;
- G. Awarding attorneys' fees and costs, as allowed by law;
- H. Awarding prejudgment and post-judgment interest, as provided by law;
- I. Granting Plaintiff and the Class leave to amend this petition to conform to the evidence produced at trial; and
- J. Granting such other or further relief as may be appropriate under the circumstances.

JURY DEMAND

Plaintiffs hereby demand that this matter be tried before a jury.

Dated: February 4, 2025

Respectfully submitted,

/s/John F. Garvey

John F. Garvey #35879

Colleen Garvey #72809

Ellen Thomas #73043

STRANCH, JENNINGS & GARVEY, PLLC

701 Market Street, Ste. 1510

St. Louis, MO 63101

Telephone: (314) 390-6750

Facsimile: (314) 255-5419

jgarvey@stranchlaw.com

cgarvey@stranchlaw.com

ethomas@stranchlaw.com

Raina Borrelli*

Stephen Pigozzi

STRAUSS BORRELLI PLLC

One Magnificent Mile

980 N. Michigan Avenue, Suite 1610

Chicago, IL 60611

Telephone: (872) 263-1100

Facsimile: (872) 263-1109

raina@straussborrelli.com

spigozzi@straussborrelli.com

** Pro hac vice forthcoming*

Attorneys for Plaintiffs and the Proposed Class