IN THE DISTRICT COURT OF OKLAHOMA COUNTY
STATE OF OKLAHOMA

WADE QUICK and **LAURA LANCE** and, individually and on behalf of all others similarly situated,

Plaintiffs,

v.

EMERGENCY MEDICAL SERVICES AUTHORITY,

Defendant.

Case No. CJ-2024-2470

Judge: Bonner

Consolidated with Case Number:

Case No. CJ-2024-2870

JURY TRIAL DEMANDED

CONSOLIDATED CLASS ACTION PETITION

Plaintiffs Wade Quick and Laura Lance (collectively, "Plaintiffs"), individually and on behalf of all other similarly situated individuals (the "Class" or "Class Members," as defined below), by and through their undersigned counsel, file this Consolidated Class Action Petition against Defendant Emergency Medical Services Authority ("EMSA" or "Defendant") and allege the following based on personal knowledge of facts, upon information and belief, and based on the investigation of their counsel as to all other matters.

I. NATURE OF THE ACTION

1. Plaintiffs bring this class action lawsuit against EMSA for its negligent failure to protect and safeguard Plaintiffs' and Class Members' highly sensitive personally identifiable information ("PII") and protected health information ("PHI") (together,

"Private Information"), culminating in a massive and preventable data breach (the "Data Breach" or "Breach") impacting at least **611,743** individuals.[1]

2. As a result of EMSA's negligence and deficient data security practices, cybercriminals easily infiltrated EMSA's inadequately protected computer systems and **stole** the Private Information of Plaintiffs and Class Members—at least **611,743** individuals.[2]

3. According to EMSA, on February 13, 2024, EMSA identified suspicious activity on its IT network.[3]

4. After an investigation, EMSA learned that an unauthorized party had gained access to its network and, between February 10, 2024, and February 13, 2024, **acquired files** that contained information pertaining to certain EMSA patients and employees.[4]

5. In other words, EMSA has already confirmed that Plaintiffs' and the Class's Private Information was **stolen** in the Data Breach.

6. The stolen information varies by individual, but generally included one or more of the following: name, address, date of birth, dates of service, name of primary care provider, and/or Social Security number.[5]

---

[1] *See* https://www.newson6.com/story/65fe2ae58a6233064cd30731/emsa-notifies-patients-of-recent-network-hack.
[2] *See* https://emsaonline.com/news/cyber-security-notice/; https://www.hipaajournal.com/benefytt-emsa-lindsay-municipal-hospital-affected-by-cyberattacks/.
[3] *See* https://emsaonline.com/news/cyber-security-notice/.
[4] *Id*.; Exs. 1–2 (Plaintiffs' Notice Letters).
[5] *See* https://emsaonline.com/news/cyber-security-notice/.

7. The victims of the Data Breach include current and former EMSA patients and employees.[6]

8. To date, there is no indication that EMSA has made any attempt to recover Plaintiffs' and Class Members' Private Information from the perpetrator of the Data Breach.

9. Because it is confirmed that Private Information was exfiltrated and acquired by cybercriminals during the Data Breach, there is no dispute that Plaintiffs' and Class Members' Private Information is in the hands of cybercriminals. As a result, Plaintiffs and Class Members will be exposed to the risk that their stolen Private Information will be used for nefarious purposes for the rest of their lives.

10. Due to EMSA's negligent failure to secure and protect Plaintiffs' and Class Members' Private Information, cybercriminals have stolen and obtained everything they need to commit identity theft and wreak havoc on the financial and personal lives of thousands of individuals.

11. Now and for the rest of their lives, Plaintiffs and the Class Members will have to deal with the danger of identity thieves possessing and misusing their Private Information. Even those Class Members who have yet to experience identity theft must spend time responding to the Data Breach and are at an immediate and heightened risk of all manner of identity theft as a direct and proximate result of the Data Breach.

[6] https://emsaonline.com/news/cyber-security-notice/; *see* Exs. 1–2.

12. Plaintiffs and Class Members have incurred and will continue to incur damages including identity theft, attempted identity theft, loss of time and money spent mitigating harms, increased risk of harm, damaged credit, diminution of the value of their Private Information, loss of privacy, and additional damages as described below.

13. Plaintiffs bring this action individually and on behalf of the Class, seeking compensatory damages, punitive damages, nominal damages, restitution, injunctive and declaratory relief, reasonable attorneys' fees and costs, and all other remedies this Court deems just and proper.

II. THE PARTIES

14. Plaintiff **Wade Quick** is an individual domiciled in the State of Oklahoma, who is a former employee of EMSA and a victim of the Data Breach.[7] Plaintiff Quick received a Notice of Data Breach Letter ("Notice Letter") from Defendant.[8]

15. Plaintiff **Laura Lance** is an individual domiciled in the State of Oklahoma who was a patient of EMSA and a victim of the Data Breach.[9] Plaintiff Lance received a Notice Letter from Defendant.[10]

16. Defendant **EMSA** is a public trust of the State of Oklahoma.

III. JURISDICTION AND VENUE

17. This action arises under the authority vested in this Court by virtue of 12 O.S. § 2004(F).

---

[7] *See* Ex. 1.
[8] *Id.*
[9] *See* Ex. 2.
[10] *Id.*

18. This Court has personal jurisdiction over EMSA because EMSA is a public trust of the State of Oklahoma, has substantial contacts with Oklahoma County, Oklahoma, and purposefully availed itself of the laws and Courts in Oklahoma County, Oklahoma.

19. Venue is proper in Oklahoma County, Oklahoma, because Defendant provides services to patients and conducts a substantial amount of business in this county. Additionally, a substantial part of the events giving rise to this action occurred in Oklahoma County, Oklahoma. Defendant also maintains Plaintiffs' and Class Members' Private Information in Oklahoma County, Oklahoma, and has caused harm to Plaintiffs and Class Members located in Oklahoma County, Oklahoma.

20. Venue is proper because EMSA is a public trust of the State of Oklahoma and is headquartered in Oklahoma.

IV. FACTUAL ALLEGATIONS

A. EMSA Collected Plaintiffs' and Class Members' Private Information.

21. EMSA is Oklahoma's largest provider of pre-hospital emergency medical care.[11]

22. EMSA was established as a not-for-profit public trust authority in Tulsa in 1977. [12]

23. In 1990, Oklahoma City joined the EMSA system, creating what is now known as EMSA's Western (Oklahoma City area) and Eastern (Tulsa area) Divisions.[13]

---

[11] https://emsaonline.com/about/.
[12] *Id.*
[13] *Id.*

24. EMSA is a public trust of the Tulsa and Oklahoma City governments.[14]

25. EMSA is overseen by an 11-member Board of Trustees, with eight of the 11 trustees appointed by the mayors of Tulsa and Oklahoma City.[15]

26. In addition to appointing individuals to serve on the EMSA Board of Trustees, the cities where EMSA operates must approve any changes to the EMSA Trust Agreement, which governs EMSA's operations.[16] The cities of cities of Tulsa and Oklahoma City approve EMSA's budget and manage the "EMSAcare" utility bill subscription program.[17]

27. An independent Medical Director provides medical oversight of the EMSA system and first responders who assist with patient assessment and stabilization.[18]

28. EMSA owns ambulances and other capital equipment used to provide service, manages contractual agreements, maintains patient records, bills and collects, purchases goods and services, works with the cities of Tulsa and Oklahoma City to administer the "EMSAcare" ambulance subscription program and makes policy recommendations.[19]

29. EMSA generated approximately $83 million in annual revenue in 2022.[20] This makes it apparent EMSA could have afforded to implement adequate data security

---

[14] *Id.*
[15] *Id.*
[16] *Id.*
[17] *Id.*
[18] *Id.*
[19] *Id.*
[20] *Id.*

prior to the Data Breach but deliberately chose not to.

30. In the ordinary course of its business, EMSA receives and stores the Private Information of thousands of patients and employees, including Plaintiffs and Class Members.

31. EMSA solicits, collects, uses, and derives a benefit from Plaintiffs' and Class Members' Private Information.

32. EMSA uses the Private Information it solicits, collects, and stores to provide healthcare services and/or employment, deriving a financial benefit therefrom.

33. EMSA would be unable to engage in its regular business activities without collecting and aggregating Private Information that it knows and understands to be sensitive and confidential.

34. Class Members who are current and former patients of EMSA, including Plaintiff Lance, paid EMSA for medical services. EMSA promised data security to its patients as part of this transaction, and part of the money it received should have been specifically allocated to providing adequate data security.

35. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' Private Information, EMSA assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiffs' and Class Members' Private Information from unauthorized disclosure.

36. EMSA recognized its duty to protect and safeguard Plaintiffs' and Class Members' Private Information and made the following claim on its website regarding its

protection of sensitive data: "The Emergency Medical Services Authority is committed to protecting the confidentiality and security of our patients' information."[21]

37. Contrary to its representations, however, EMSA failed to implement adequate data security measures to protect Plaintiffs' and Class Members' Private Information, resulting in a devastating data breach that affected more than 600,000 people.

B. EMSA's Massive and Preventable Data Breach.

38. According to EMSA, on February 13, 2023, EMSA identified suspicious activity on its IT Network.[22]

39. After discovering the intrusion, EMSA claims it initiated its response protocols, which involved shutting off select systems as a proactive measure.[23]

40. After an investigation, EMSA confirmed that the highly sensitive Private Information of Plaintiffs and the Class had been stolen during the Data Breach: "The investigation determined that an unauthorized party gained access to our network and, between February 10, 2024, and February 13, 2024, **acquired files** that contained information pertaining to certain EMSA patients."[24]

41. The information stolen in the Data Breach included the names, addresses, dates of birth, dates of service, names of primary care providers, and Social Security numbers of current and former EMSA patients and employees.[25]

---

[21] https://emsaonline.com/news/cyber-security-notice/.
[22] *Id.*
[23] *Id.*
[24] *Id.* (emphasis added).
[25] *Id.*

42. Despite learning of the Data Breach on February 13, 2023, EMSA inexplicably waited to notify Plaintiffs and the Class of the Data Breach until on or around March 22, 2024, when it began sending Notice of Data Breach Letters ("Notice Letter") to victims of the Data Breach.[26]

43. EMSA also posted the following notice on its website:[27]

[IMAGE ON NEXT PAGE]

[26] *See* Exs. 1–2.
[27] https://emsaonline.com/news/cyber-security-notice/.

Cyber Security Incident Notice to Our Patients

A Notice to Our Patients

The Emergency Medical Services Authority is committed to protecting the confidentiality and security of our patients' information. Regrettably, we recently identified and addressed a security incident that involved some of that information.

On February 13, 2024, EMSA identified suspicious activity in our IT network. We immediately initiated our incident response protocols, which involved shutting off select systems as a proactive measure. We also launched an investigation with the assistance of a third-party forensic firm and notified law enforcement. The investigation determined that an unauthorized party gained access to our network and, between February 10, 2024 and February 13, 2024, acquired files that contained information pertaining to certain EMSA patients. The information involved varied by individual, but generally included one or more of the following: name, address, date of birth, date of service, and, for some, name of primary care provider and/or Social Security number.

As a precaution, we are mailing notification letters to patients whose information may have been involved and for whom we have sufficient contact information. We have also established a dedicated, toll-free call center to answer questions about the incident. If you have questions, please call (866) 495-7098, available Monday through Friday, from 8:00 a.m. to 5:30 p.m. Central Time. We are providing individuals whose Social Security numbers were involved with a complimentary offer to credit monitoring and identity protection support services. Additionally, we'd like to remind patients that it is always a good idea to carefully review the communications they receive from their healthcare providers, including electronic messages, billing statements, and other written communication. If patients see charges for services they did not receive, they should contact the issuing provider immediately.

To help prevent something like this from happening again, we have implemented, and will continue to adopt, additional safeguards to further protect and monitor our systems.

44. Omitted from the Notice Letter were the date(s) of EMSA's investigation, an explanation as to why EMSA failed to inform Plaintiffs and Class Members of the Data Breach's occurrence for *more than a month* after detecting the cyberattack, the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures, if any, undertaken to ensure that such a breach does not occur again. To date, these critical

facts still have not been provided to Plaintiffs and Class Members, who retain a vested interest in ensuring that the Private Information in Defendant's possession is protected.

45. The Notice Letter provided by EMSA amounts to no real disclosure at all, as it fails to inform Plaintiffs and Class Members of critical facts concerning the Data Breach with any degree of specificity. Without these details, Plaintiffs' and Class Members' ability to mitigate the harms resulting from the Data Breach is severely diminished.

46. EMSA failed to take the necessary precautions required to safeguard and protect Plaintiffs' and Class Members' Private Information from unauthorized access and exploitation.

47. EMSA also failed to timely notify Plaintiffs and Class Members of the Data Breach.

48. EMSA's actions represent a flagrant disregard of the rights of Plaintiffs and the Class, both as to privacy and property.

49. As such, Plaintiffs and the Class continue to be at imminent and impending risk of identity theft and fraud.

C. Cybercriminals Will Use Plaintiffs' and Class Members' Private Information to Defraud them.

50. Private Information is of great value to hackers and cybercriminals, and the data stolen in the Data Breach can and will be used in a variety of ways to exploit Plaintiffs and Class Members and to profit off their misfortune.

51. Each year, identity theft causes tens of billions of dollars of losses to victims in the United States.[28]

52. For example, with the Private Information stolen in the Data Breach, including Social Security numbers, identity thieves can open financial accounts, apply for credit, obtain medical services, file fraudulent tax returns, commit crimes, create false driver's licenses and other forms of identification and sell them to other criminals or undocumented immigrants, steal government benefits, give breach victims' names to police during arrests, and many other harmful forms of identity theft.[29]

53. These criminal activities have resulted and will continue to cause devastating financial and personal losses to Plaintiffs and Class Members.

54. Medical-related identity theft is one of the most common, most expensive forms of identity theft, and it's one of the most difficult to prevent. According to Kaiser Health News, "medical-related identity theft accounted for 43 percent of all identity thefts reported in the United States in 2013[,]" which is more than identity thefts involving banking and finance, the government and the military, or education.[30]

55. "Medical records are a gold mine for criminals—they can access a patient's name, DOB, Social Security and insurance numbers, and even financial information all in

---

[28] *Facts + Statistics: Identity Theft and Cybercrime*, INSURANCE INFO. INST., https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (last visited April 11, 2024).

[29] *See, e.g.*, Nikkita Walker, *What Can You Do With Your Social Security Number*, CREDIT.COM (Oct. 19, 2023), https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/.

[30] Michael Ollove, *The Rise of Medical Identity Theft in Healthcare*, KAISER HEALTH NEWS (Feb. 7, 2014), https://khn.org/news/rise-of-indentity-theft/.

one place."[31] A complete identity theft kit that includes health insurance credentials may be worth up to $1,000 on the black market.[32]

56. When cybercriminals manage to steal health insurance information and other personally sensitive data—as they did here—there is no limit to the amount of fraud to which Plaintiffs and Class Members are exposed.

57. Social Security numbers are particularly sensitive pieces of personal information. As the Consumer Federation of America explains:

> **Social Security number.** *This is the most dangerous type of personal information in the hands of identity thieves* because it can open the gate to serious fraud, from obtaining credit in your name to impersonating you to get medical services, government benefits, your tax refunds, employment – even using your identity in bankruptcy and other legal matters. It's hard to change your Social Security number and it's not a good idea because it is connected to your life in so many ways.[33]
>
> (Emphasis added.)

58. PII is such a valuable commodity to identity thieves that once it has been compromised, criminals will use it for years.[34]

---

[31] *You Got It, They Want It: Criminals Targeting Your Private Healthcare Data, New Ponemon Study Shows*, IDX (May 14, 2015) https://www.idx.us/knowledge-center/you-got-it-they-want-it-criminals-are-targeting-your-private-healthcare-dat..

[32] *Managing cyber risks in an interconnected world: Key findings from The Global State of Information Security Survey 2015*, PRICEWATERHOUSECOOPERS (Sept. 30, 2014), https://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf.

[33] *Dark Web Monitoring: What You Should Know*, CONSUMER FEDERATION OF AMERICA (Mar. 19, 2019), https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/.

[34] *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO (July 5, 2007), https://www.gao.gov/products/gao-07-737.

59. The Data Breach at issue here was targeted and financially motivated, as the only reason cybercriminals go through the trouble of hacking companies like EMSA is to steal the highly sensitive information they maintain, which can be exploited and sold for use in the kinds of criminal activity described herein.

60. A Social Security number, date of birth, and full name can sell for $60 to $80 on the digital black market.[35]

61. PHI is even more valuable on the black market than PII.[36]

62. According to the Center for Internet Security, "[t]he average cost of a data breach incurred by a non-healthcare related agency, per stolen record, is $158. For healthcare agencies the cost is an average of $355. Credit card information and PII sell for $1-$2 on the black market, but PHI can sell for as much as $363 according to the Infosec Institute. This is because one's personal health history, including ailments, illnesses, surgeries, etc., can't be changed, unlike credit card information or Social Security Numbers."[37]

63. "PHI is valuable because criminals can use it to target victims with frauds and scams that take advantage of the victim's medical conditions or victim settlements. It can also be used to create fake insurance claims, allowing for the purchase and resale of

---

[35] Michael Kan, *Here's How Much Your Identity Goes for on the Dark Web*, PGMAG (Nov. 15, 2017), https://www.pcmag.com/news/heres-how-much-your-identity-goes-for-on-the-dark-web.
[36] *Data Breaches: In the Healthcare Sector*, CENTER FOR INTERNET SECURITY, https://www.cisecurity.org/insights/blog/data-breaches-in-the-healthcare-sector (last visited April 11, 2024).
[37] *Id.*

medical equipment. Some criminals use PHI to illegally gain access to prescriptions for their own use or resale."[38]

64. Identity theft experts advise victims of data breaches: "[I]f there is reason to believe that your personal information has been stolen, you should assume that it can end up for sale on the dark web."[39]

65. The risks of identity fraud are both certainly impending and substantial. As the Federal Trade Commission ("FTC") has reported, if hackers get access to PII, **they will use it**.[40]

66. Hackers may not use the information right away, but this does not mean it will not be used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information **may continue for years**. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[41]

---

[38] *Id.*

[39] *Dark Web Monitoring: What You Should Know*, CONSUMER FEDERATION OF AMERICA (Mar. 19, 2019), https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/.

[40] Ari Lazarus, *How fast will identity thieves use stolen info?*, MILITARY CONSUMER (May 24, 2017), https://www.militaryconsumer.gov/blog/how-fast-will-identity-thieves-use-stolen-info.

[41] *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO (July 5, 2007), https://www.gao.gov/products/gao-07-737 (emphasis added).

67. For instance, with a stolen Social Security number, which is part of the Private Information compromised in this Data Breach, criminals can open financial accounts, get medical care, file fraudulent tax returns, commit crimes, and steal benefits.[42]

68. Identity theft victims must spend countless hours and large amounts of money repairing the impact to their credit as well as protecting themselves in the future.[43]

69. EMSA made a limited offering of identity monitoring to Plaintiffs and the Class. Such coverage is woefully inadequate and will not fully protect Plaintiffs and the Class from the damages and harm caused by EMSA's negligent failure to secure and protect their Private Information.

70. The unfortunate truth is the full scope of the harm has yet to be realized. There may be a time lag between when harm occurs and when it is discovered, and also between when Private Information is stolen and when it is used.

71. Plaintiffs and Class Members will need to pay for their own identity theft protection and credit monitoring for the rest of their lives, owing to EMSA's negligence.

72. Furthermore, identity monitoring services only alert someone to the fact that they have already been the victim of identity theft—these services do not prevent identity theft.[44]

---

[42] *See* Nikkita Walker, *What Can Someone Do with Your Social Security Number?*, CREDIT.COM (Oct. 19, 2023), https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/.

[43] *Guide for Assisting Identity Theft Victims*, FEDERAL TRADE COMMISSION (Sept. 2013), https://www.global-screeningsolutions.com/Guide-for-Assisting-ID-Theft-Victims.pdf.

[44] *See* Kayleigh Kulp, *Credit monitoring services may not be worth the cost*, CNBC (Nov. 30, 2017, 9:00 AM), https://www.cnbc.com/2017/11/29/credit-monitoring-services-may-not-be-worth-the-cost.html.

73. Nor can an identity monitoring service remove personal information from the dark web.[45]

74. "The people who trade in stolen personal information [on the dark web] won't cooperate with an identity theft service or anyone else, so it's impossible to get the information removed, stop its sale, or prevent someone who buys it from using it."[46]

75. As a direct and proximate result of the Data Breach, Plaintiffs and the Class have been damaged and placed at an imminent and continuing increased risk of harm from fraud and identity theft. Plaintiffs and the Class must now take the time and effort to mitigate the actual and potential impact of the Data Breach on their everyday lives, including placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts, credit reports, and medical records for unauthorized activity for years to come. The time they are required to spend as a result of the Data Breach is time lost to spend on other productive activities in their lives.

76. Even more serious is the identity restoration that Plaintiffs and other Class Members must go through, which can require spending countless hours filing police reports, filling out IRS forms, completing Federal Trade Commission checklists and Department of Motor Vehicle driver's license replacement applications, and calling

[45] *Dark Web Monitoring: What You Should Know*, CONSUMER FEDERATION OF AMERICA (Mar. 19, 2019), https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/.
[46] *Id.*

financial institutions to cancel fraudulent credit applications, to name just a few of the steps Plaintiffs and the Class must take.

77. Plaintiffs and the Class have or will experience the following concrete and particularized harms for which they are entitled to compensation, including:

a. Actual identity theft;

b. Trespass, damage to, and theft of their personal property, including their Private Information;

c. Improper disclosure and theft of their Private Information;

d. The imminent and certainly impending injury flowing from potential fraud and identity theft posed by their Private Information being placed in the hands of criminals;

e. Loss of privacy suffered as a result of the Data Breach, including the harm of knowing cybercriminals have their Private Information;

f. Ascertainable losses in the form of time taken to respond to identity theft, including lost opportunities and lost wages from uncompensated time off from work;

g. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably expended to remedy or mitigate the effects of the Data Breach;

h. Ascertainable losses in the form of diminution of the value of Plaintiffs' and Class Members' Private Information, for which there is a well-established and quantifiable national and international market;

i. The loss of use of and access to their credit, accounts, and/or funds;

j. Damage to their credit due to fraudulent use of their Private Information; and/or

k. Increased cost of borrowing, insurance, deposits, and the inability to secure more favorable interest rates because of a reduced credit score.

78. Moreover, Plaintiffs and Class Members have an interest in ensuring that their Private Information, which remains in the possession of Defendant, is protected from further breaches through the implementation of industry-standard security measures and safeguards. Defendant has shown itself wholly incapable of protecting Plaintiffs' and Class Members' Private Information.

79. Plaintiffs and Class Members also have an interest in ensuring that their Private Information is removed from all EMSA servers, systems, and files.

80. The notice provided by EMSA acknowledged that the Data Breach would cause harm to affected individuals and that financial harm would likely occur.[47]

81. At EMSA's specific recommendation, Plaintiffs are desperately trying to mitigate the damages EMSA caused them. [48]

[47] *See* Exs. 1–2.
[48] *Id*.

82. Given the kind of Private Information EMSA made accessible to hackers, however, Plaintiffs are certain to incur additional damages. Because identity thieves have their Private Information, Plaintiffs and Class Members will need to have identity theft monitoring protection for the rest of their lives. Some may even need to go through the long and arduous process of getting a new Social Security number, with all the complications—including loss of credit and employment difficulties—that come with a new number.[49]

83. None of these privacy injuries should have happened, because the Data Breach was entirely preventable.

D. EMSA was Aware of the Risk of Cyberattacks.

84. According to the Center for Internet Security, "the health industry experiences more data breaches than any other sector."[50] This is because "Personal Health Information (PHI) is more valuable on the black market than credit card credentials or regular Personally Identifiable Information (PII). Therefore, there is a higher incentive for cyber criminals to target medical databases. They can sell the PHI and/or use it for their own personal gain."[51]

85. "In 2023, more than 540 organizations and 112 million individuals were

---

[49] *What happens if I change my Social Security number?*, LEXINGTON LAW (Aug. 10, 2022), https://www.lexingtonlaw.com/blog/credit-101/will-a-new-social-security-number-affect-your-credit.html.

[50] *Data Breaches: In the Healthcare Sector*, CENTER FOR INTERNET SECURITY, https://www.cisecurity.org/insights/blog/data-breaches-in-the-healthcare-sector (last visited April 11, 2024).

[51] *Id.*

implicated in healthcare data breaches reported to the HHS Office for Civil Rights (OCR), compared to 590 organizations and 48.6 million impacted individuals in 2022."[52]

86. "The number of cybersecurity attacks disrupting the healthcare sector has continued to be a growing concern. In the last three years, more than 90% of all healthcare organizations have reported at least one security breach which can manifest in denial of service, malicious code, ransomed data, and more."[53]

87. "Healthcare organi[z]ations are rich targets for cybercriminals because they hold a large amount of sensitive patient data. This data can be used to commit identity theft or fraud or sold on the black market. Hackers can access this data in many ways, including phishing emails, malware, and unsecured networks."[54]

88. It is no secret that "[h]ealthcare data breaches are reaching record highs. Indeed, healthcare now sees more cyberattacks than any other industry. Fully one-third of all cyberattacks are aimed at healthcare institutions. Why? Because healthcare is a valuable and vulnerable target. Hospitals and healthcare institutions are a prime target for cybercrime due to the vast amount of sensitive data they hold."[55]

89. The health industry is frequently recognized as one of the most vulnerable

---

[52] *This Year's Largest Healthcare Data Breaches*, HEALTH IT SECURITY (Dec. 26, 2023), https://healthitsecurity.com/features/this-years-largest-healthcare-data-breaches.

[53] *6 Industries Most Vulnerable to Cyber Attacks*, WGU (Aug. 3, 2021), https://www.wgu.edu/blog/6-industries-most-vulnerable-cyber-attacks2108.html.

[54] Troy Beamer, *What Industries Are Most Vulnerable to Cyber Attacks In 2024?*, TECHNEWS (Feb. 27, 2024), https://www.techbusinessnews.com.au/what-industries-are-most-vulnerable-to-cyberattacks-in-2022/.

[55] *What Industries Are Most Vulnerable to Cyberattacks?*, PSM, https://www.psmpartners.com/blog/most-targeted-industries-for-cyber-attacks/ (last accessed April 11, 2024).

industries for a cyberattack.[56]

90. EMSA should have been aware, and indeed was aware, that it was at risk of a data breach that could expose the Private Information that it solicited, collected, stored, and maintained, especially given the rise of healthcare data breaches.

91. EMSA's assurances to patients that it maintains high standards of cybersecurity are further evidence that EMSA recognized it had a duty to use reasonable measures to protect the Private Information that it solicited, collected, and maintained.

92. EMSA was aware of the risks and harm that could result from inadequate data security.

E. EMSA Could Have Prevented the Data Breach.

93. Data breaches, including EMSA's, are preventable.[57] "In almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions."[58] "Organizations that

[56] *See, e.g.*, *id.*; Liudmyla Pryimenko, *The 7 Industries Most Vulnerable to Cyberattacks*, EKRAN (Mar. 25, 2024), https://www.ekransystem.com/en/blog/5-industries-most-risk-of-data-breaches; Ani Petrosyan, *Distribution of cyberattacks across worldwide industries in 2023*, STATISTA (Mar. 22, 2024), https://www.statista.com/statistics/1315805/cyber-attacks-top-industries-worldwide/; *6 Industries Most Vulnerable to Cyber Attacks*, WGU (Aug. 3, 2021), https://www.wgu.edu/blog/6-industries-most-vulnerable-cyber-attacks2108.html.

[57] Lucy L. Thomson, *Despite the Alarming Trends, Data Breaches Are Preventable*, DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012), available at https://lawcat.berkeley.edu/record/394088.

[58] *Id.* at 17.

collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised[.]"[59]

94. Most reported data breaches "are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures. . . . Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a *data breach never occurs*."[60]

95. Here, many failures laid the groundwork for EMSA's Data Breach.

96. The FTC has published guidelines that establish reasonable data security practices for businesses.[61]

97. The FTC guidelines emphasize the importance of having a data security plan, regularly assessing risks to computer systems, and implementing safeguards to control such risks.[62]

98. The FTC guidelines establish that businesses should protect the confidential information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies for installing vendor-approved patches to correct security problems.[63]

---

[59] *Id.* at 28.
[60] *Id.*
[61] *Protecting Personal Information: A Guide for Business*, FTC (Oct. 2016), available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.
[62] *Id.*
[63] *Id.*

99. The FTC guidelines also recommend that businesses utilize an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating hacking attempts; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[64]

100. According to information and belief, EMSA failed to follow reasonable and necessary industry standards to prevent a data breach, including the FTC's guidelines.

101. Based upon information and belief, EMSA also failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework, NIST Special Publications 800-53, 53A, or 800-171; the Federal Risk and Authorization Management Program (FEDRAMP); or the Center for Internet Security's Critical Security Controls (CIS CSC), which are well respected authorities in cybersecurity readiness.

102. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[65]

103. To prevent and detect the attack here, EMSA could and should have taken, as recommended by the Federal Bureau of Investigation, the following measures:

- Implemented an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.

---

[64] *Id.*

[65] *See How to Protect Your Networks from RANSOMWARE*, at 3, available at https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view.

- Enabled strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scanned all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configured firewalls to block access to known malicious IP addresses.
- Patched operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Managed the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configured access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.

- Disabled macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implemented Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.
- Considered disabling Remote Desktop protocol (RDP) if it is not being used.
- Used application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Executed operating system environments or specific programs in a virtualized environment.
- Categorized data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[66]

104. According to information and belief, EMSA failed to do any of the above.

[66] *Id.* at 3–4.

105. To prevent and detect ransomware attacks, EMSA could and should have instructed its employees, as recommended by the United States Cybersecurity & Infrastructure Security Agency, to take the following measures:

- **Update and patch their computers**. Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks.
- **Use caution with links and when entering website addresses**. Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net).
- **Open email attachments with caution**. Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.
- **Keep their personal information safe**. Check a website's security to ensure the information you submit is encrypted before you provide it.

- **Verify email senders**. If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.
- **Inform yourself**. Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.
- **Use and maintain preventative software programs**. Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic.[67]

106. In addition, to prevent and detect a data breach, including the one that occurred here, EMSA could and should have implemented the following measures, as recommended by the Microsoft Threat Protection Intelligence Team:

- **Harden internet-facing assets**
    - Apply latest security updates

[67] *See Protecting Against Ransomware*, CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY (revised Sept. 2, 2021), https://www.cisa.gov/news-events/news/protecting-against-ransomware (internal citations omitted).

- Use threat and vulnerability management
- Perform regular audits

- **Thoroughly investigate and remediate alerts.**
  - Prioritize and treat commodity malware infections as potential full compromise of the system
- **Include IT professionals in security discussions.**
  - Ensure collaboration among security operations, security administrators, and information technology administrators to configure servers and other endpoints securely
- **Build and maintain credential hygiene**
  - Use multifactor authentication or network level authentication and enforce strong, randomized, just-in-time local administrator passwords
- **Apply the principle of least-privilege**
  - Monitor for adversarial activities
  - Hunt for brute force attempts
  - Monitor for cleanup of Event Logs
  - Analyze logon events
- **Harden infrastructure**
  - Utilize Windows Defender Firewall
  - Enable tamper protection

- Enable cloud-delivered protection
- Turn on attack surface reduction rules and Antimalware Scan Interface for Office Visual Basic for Applications[68]

107. Given that EMSA was storing the Private Information of thousands of individuals, EMSA could and should have implemented all the above measures to prevent and detect cyberattacks.

108. However, EMSA failed to implement proper security measures. Specifically, among other failures, EMSA had far too much confidential information held unencrypted on its systems. Such Private Information should have been segregated into an encrypted system.[69]

109. Moreover, it is well-established industry standard practice to dispose of confidential Private Information once it is no longer needed.[70]

110. The FTC has repeatedly emphasized the importance of disposing of unnecessary Private Information: "Keep sensitive data in your system only as long as you have a business reason to have it. Once that business need is over, properly dispose of it. If it's not on your system, it can't be stolen by hackers."[71] Rather than following this basic

---

[68] *See Human-operated ransomware attacks: A preventable disaster*, MICROSOFT THREAT INTELLIGENCE (Mar 5, 2020), https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/.
[69] *See* Adnan Raja, *How to Safeguard Your Business Data With Encryption*, DATAINSIDER (Aug. 14, 2018), https://digitalguardian.com/blog/how-safeguard-your-business-data-encryption.
[70] *See Protecting Personal Information: A Guide for Business*, FEDERAL TRADE COMMISSION (Oct. 2016), https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business.
[71] *Id.* at 6.

standard of care, EMSA kept millions of individuals' unencrypted Private Information on their inadequately secured systems indefinitely.

111. In sum, the Data Breach could have been easily prevented through standard practices such as the use of network segmentation and encryption of all Private Information—which EMSA negligently failed to do.

112. Further, the scope of the Data Breach could have been dramatically reduced had EMSA utilized proper record retention and destruction practices—but EMSA negligently did no such thing.

F. EMSA had an Obligation to Protect Private Information Under the Law and the Applicable Standard of Care.

113. As a healthcare service provider handling patients' medical data and providing services to hospitals and healthcare organizations, EMSA is a covered entity under HIPAA (45 C.F.R. § 160.103). As such, EMSA is required to comply with the HIPAA Privacy Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and the HIPAA Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and C ("Security Standards for the Protection of Electronic Protected Health Information").

114. HIPAA's Privacy Rule establishes national standards for protecting health information, including health information that is kept or transferred in electronic form.

115. EMSA is required to "comply with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302.

116. "Electronic protected health information" is "individually identifiable health information . . . that is: (i) transmitted by electronic media; [or] (ii) maintained in electronic media[.]" 45 C.F.R. § 160.103.

117. The HIPAA Security Rule, 45 C.F.R. Part 164, Subpart C, requires EMSA to:

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

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; and

d. Ensure compliance by its workforce.

118. HIPAA also requires EMSA 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).

119. Additionally, HIPAA requires EMSA 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).

120. The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, further requires EMSA to provide notice of the Data Breach to each affected individual "without unreasonable delay and in no case later than 60 days following discovery of [the] breach[.]"

121. EMSA was also prohibited by the Federal Trade Commission Act, 15 U.S.C. § 45 (the "FTC Act"), from engaging in "unfair or deceptive acts or practices in or affecting commerce[.]" The FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. *See, e.g.*, *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

122. EMSA is further required by various states' laws and regulations to protect Plaintiffs' and Class Members' Private Information.

123. EMSA owed a duty to Plaintiffs and the Class to design, maintain, and test its computer and email systems to ensure that the Private Information in its possession and control was adequately secured and protected.

124. EMSA owed a duty to Plaintiffs and the Class to create and implement reasonable data security practices and procedures to protect the Private Information in its possession, including adequately training its employees (and any others who accessed Private Information within its computer systems) on how to protect Private Information.

125. EMSA owed a duty to Plaintiffs and the Class to implement processes that would detect a breach of its data security systems in a timely manner.

126. EMSA owed a duty to Plaintiffs and the Class to act upon data security warnings and alerts in a timely fashion.

127. EMSA owed a duty to Plaintiffs and the Class to adequately train and supervise its employees to identify and avoid any phishing emails that make it past its email filtering service.

128. EMSA owed a duty to Plaintiffs and the Class to disclose if their computer systems and data security practices were inadequate to safeguard individuals' Private Information from theft, because such an inadequacy would be a material fact in individuals' decisions to entrust EMSA with their Private Information.

129. EMSA owed a duty to Plaintiffs and the Class to disclose in a timely and accurate manner when data breaches occurred.

130. EMSA owed a duty of care to Plaintiffs and the Class because they were foreseeable and probable victims of any inadequate data security practices.

G. Plaintiffs' Individual Experiences

i. *Plaintiff Wade Quick*

131. Plaintiff Quick entrusted his Private Information to EMSA as an employee of EMSA with the reasonable expectation and mutual understanding that EMSA would keep his Private Information secure from unauthorized access. Had Plaintiff Quick been aware that EMSA's computer systems were not secure, he would not have entrusted EMSA with his PII and PHI.

132. By soliciting and accepting Plaintiff Quick's Private Information, EMSA agreed to safeguard and protect it from unauthorized access and delete it after a reasonable

time.

133. EMSA was in possession of Plaintiff Quick's Private Information before, during, and after the Data Breach.

134. After the Data Breach, Plaintiff Quick received a Notice Letter from EMSA, notifying him that an unauthorized party gained access to EMSA's network between February 10, 2024, and February 13, 2024, and "acquired files that contained information pertaining to certain current and former EMSA employees," which included his name and Social Security number.[72]

135. After receiving the Notice Letter, Plaintiff Quick made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to researching the Data Breach, reviewing and monitoring his accounts for fraudulent activity, and reviewing his credit reports. In total, Plaintiff Quick estimates he has already spent **hours** responding to the Data Breach.

136. Plaintiff Quick will be forced to expend additional time to review his credit reports and monitor his accounts for the rest of his life. This time, spent at Defendant's direction, has been lost forever and cannot be recaptured.

137. Plaintiff Quick places significant value in the security of his Private Information and does not readily disclose it. Plaintiff Quick entrusted EMSA with his Private Information with the understanding that EMSA would keep his information secure and would employ reasonable and adequate data security measures to ensure that his

[72] Ex. 1.

Private Information would not be compromised.

138. Plaintiff Quick has never knowingly transmitted unencrypted Private Information over the internet or any other unsecured source.

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

140. Plaintiff Quick has been and will continue to be at a heightened and substantial risk of future identity theft and its attendant damages for years to come. This risk is certainly real and impending, and is not speculative, given the highly sensitive nature of the Private Information stolen in the Data Breach.[73]

141. Knowing that thieves intentionally targeted and stole his Private Information,

[73] *Id.*

and knowing that his Private Information, including his Social Security number, is now in the hands of cybercriminals has caused Plaintiff Quick great anxiety beyond mere worry. Specifically, Plaintiff Quick has lost hours of sleep, is in a constant state of stress, is very frustrated, and is in a state of persistent worry now that his Private Information has been stolen.

142. Plaintiff Quick has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains in the possession of Defendant, is protected and safeguarded from future data breaches. Absent Court intervention, Plaintiff Quick's Private Information will be wholly unprotected and at-risk of future data breaches.

ii. ***Plaintiff Laura Lance***

143. Plaintiff Laura Lance entrusted her Private Information to EMSA as a patient of EMSA with the reasonable expectation and mutual understanding that EMSA would keep her Private Information secure from unauthorized access. Had Plaintiff Lance been aware that EMSA's computer systems were not secure, she would not have entrusted EMSA with her PII and PHI.

144. By soliciting and accepting Plaintiff Lance's Private Information, EMSA agreed to safeguard and protect it from unauthorized access and delete it after a reasonable time.

145. EMSA was in possession of Plaintiff Lance's Private Information before, during, and after the Data Breach.

146. After the data breach, Plaintiff Lance received a copy of the Notice Letter

dated April 16, 2024, informing her that that an unauthorized party gained access to EMSA's network between February 10, 2024, and February 13, 2024, and "acquired files that contained information pertaining to certain current and former EMSA employees," which included her name, address, date of birth, Social Security number, dates of service, and/or name of primary care provider.[74]

147. After receiving the Notice Letter, Plaintiff Lance made reasonable efforts to mitigate the impact of the Data Breach. For instance, Plaintiff Lance has been spending about 40 minutes a week (adding up to many hours) monitoring her financial accounts, and she is in the process of changing all her passwords. This is far more time than she spent monitoring her accounts prior to the Breach, and the need to monitor so closely causes her great anxiety.

148. Plaintiff Lance will be forced to expend additional time monitoring her credit reports and accounts for the rest of her life. This time, spent at Defendant's direction, has been lost forever and cannot be recaptured.

149. Following the Data Breach, Plaintiff Lance began receiving an excessive number of spam calls, texts, and emails to the cell phone number and email address she provided to EMSA. This flood of spam is a distraction and a hassle that she must deal with on a daily basis. Given the timing of the Data Breach, she believes that the uptick of spam is related to the theft of her Private Information.

150. Plaintiff Lance places significant value in the security of her Private

[74] *See* Ex. 2.

Information and does not readily disclose it. Plaintiff Lance entrusted EMSA with her Private Information with the understanding that EMSA would keep her information secure and would employ reasonable and adequate data security measures to ensure that her Private Information would not be compromised.

151. Plaintiff Lance has never knowingly transmitted unencrypted Private Information over the internet or any other unsecured source.

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

153. Plaintiff Lance has been and will continue to be at a heightened and substantial risk of future identity theft and its attendant damages for years to come. This risk is certainly real and impending, and is not speculative, given the highly sensitive nature

of the Private Information stolen in the Data Breach.[75]

154. Knowing that thieves intentionally targeted and stole her Private Information, and knowing that her Private Information, including her Social Security number, is now in the hands of cybercriminals has caused Plaintiff Lance great anxiety beyond mere worry. Specifically, Plaintiff Lance has lost hours of sleep, is in a constant state of stress, is very frustrated, and is in a state of persistent worry now that her Private Information has been stolen.

155. Plaintiff Lance has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains in the possession of Defendant, is protected and safeguarded from future data breaches. Absent Court intervention, Plaintiff Lance's Private Information will be wholly unprotected and at risk of future data breaches.

V. CLASS ACTION ALLEGATIONS

156. Plaintiffs incorporate by reference all preceding factual paragraphs as if fully restated here.

157. Plaintiffs bring this action against EMSA on behalf of themselves and all other individuals similarly situated under 12 O.S. § 2023. Plaintiffs assert all claims on behalf of a nationwide class (the "Class") defined as follows:

> **All persons who received a Notice Letter from EMSA informing them that their PII and/or PHI was potentially compromised in EMSA's Data Breach occurring in or around February 2024.**

[75] *Id.*

158. Excluded from the Class are Defendant, any entity in which Defendant has a controlling interest, and Defendant's officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded from the Class is any judge, justice, or judicial officer presiding over this matter and members of their immediate families and their judicial staff members.

159. Plaintiffs reserve the right to amend or modify the above Class definition or to propose subclasses in subsequent pleadings and motions for class certification.

160. Plaintiffs anticipate the issuance of notice setting forth the subject and nature of the instant action to the proposed Class. Upon information and belief, Defendant's own business records or electronic media can be utilized for the notice process.

161. The proposed Class meets the requirements of 12 O.S. § 2023.

162. **Numerosity:** The proposed Class is so numerous that joinder of all members is impracticable. The total number of individuals affected is more than 600,000.

163. **Typicality:** Plaintiffs' claims are typical of the claims of the Class because Plaintiffs' Private Information, like that of every other Class Member, was compromised in the Data Breach. Plaintiffs and all members of the Class were injured by the same wrongful acts, practices, and omissions committed by EMSA, as described herein. Plaintiffs' claims therefore arise from the same practices or course of conduct that give rise to the claims of all Class Members.

164. **Adequacy:** Plaintiffs are adequate representatives of the Class because Plaintiffs' interests do not conflict with the interests of the Class. Plaintiffs have retained

counsel competent and highly experienced in data breach class action litigation, and Plaintiffs and Plaintiffs' counsel intend to prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiffs and their counsel.

165. **Superiority:** A class action is superior to other available means of fair and efficient adjudication of the claims of Plaintiffs and the Class. The injury suffered by each individual Class Member is relatively small in comparison to the burden and expense of individual prosecution of complex and expensive litigation. It would be very difficult if not impossible for individual members of the Class to effectively redress EMSA's wrongdoing. Even if Class Members could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties, and to the court system, presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties and provides benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

166. **Commonality and Predominance:** Defendant engaged in a common course of conduct toward Plaintiffs and Class Members, in that Plaintiffs' and Class Members' Private Information was stored on the same network and unlawfully accessed in the same way. There are many questions of law and fact common to the claims of Plaintiffs and those of the other members of the Class, and those questions predominate over any questions that may affect individual Class Members. Common questions for the Class include:

a. Whether Defendant engaged in the wrongful conduct alleged herein;

b. Whether Defendant owed a duty to Plaintiffs and Class Members to adequately protect their Private Information;

c. Whether Defendant breached its duty to Plaintiffs and Class Members to adequately protect their Private Information;

d. Whether Defendant failed to implement and maintain security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

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

f. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

g. Whether Defendant knew or should have known that its computer and network security systems, or the computer and network security systems of its vendors, were vulnerable to cyberattacks;

h. Whether Defendant's conduct, including its failure to act, resulted in or was the proximate cause of the Data Breach;

i. Whether Defendant was negligent in permitting Private Information belonging to millions of individuals to be stored unencrypted within its network;

j. Whether Defendant was negligent in failing to adhere to reasonable data retention policies;

k. Whether Defendant breached implied contractual duties to Plaintiffs and the Class to use reasonable care in protecting their Private Information;

l. Whether Defendant was unjustly enriched by unlawfully retaining a benefit conferred upon it by Plaintiffs and Class Members;

m. Whether Defendant should have discovered the Data Breach sooner;

n. Whether Defendant failed to adequately respond to the Data Breach, including failing to investigate it diligently and notify affected individuals in the most expedient time possible and without unreasonable delay, and whether this caused damages to Plaintiffs and the Class;

o. Whether Defendant continues to breach duties owed to Plaintiffs and the Class;

p. Whether Plaintiffs and the Class suffered injuries as a proximate result of Defendant's negligent actions or failures to act;

q. Whether Defendant was negligent in selecting, supervising, and/or monitoring vendors;

r. Whether Plaintiffs and the Class are entitled to recover damages, equitable relief, and other relief; and

s. Whether Defendant's actions alleged herein constitute gross negligence, and whether Plaintiffs and Class Members are entitled to punitive damages.

167. Defendant has acted on grounds that apply generally to the Class as a whole, so that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

168. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to Class Members' names and addresses. Class Members have already been preliminarily identified and sent notice of the Data Breach by Defendant.

VI. CAUSES OF ACTION

FIRST CAUSE OF ACTION
NEGLIGENCE
(On Behalf of Plaintiffs and the Class)

169. Plaintiffs re-allege and incorporate by reference all preceding factual paragraphs as though fully set forth herein.

170. EMSA solicited, collected, stored, and maintained the Private Information of Plaintiffs and Class Members on inadequately secured computer systems and networks.

171. Upon accepting and storing Plaintiffs' and Class Members' Private Information on its computer systems and networks, Defendant undertook and owed a duty to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting their Private Information from unauthorized access and disclosure.

172. Defendant owed a duty of care to Plaintiffs and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its computer systems and networks, and the personnel responsible for

them, adequately protected the Private Information.

173. Defendant's duty included a responsibility to implement processes by which it could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

174. Defendant had full knowledge of the sensitivity of the Private Information in its possession and the types of harm that Plaintiffs and Class Members could and would suffer if the Private Information was wrongfully accessed or disclosed. Plaintiffs and Class Members were therefore the foreseeable victims of any inadequate data security practices.

175. Defendant's duty to implement and maintain reasonable data security practices arose as a result of the special relationship that exists between Defendant and consumers, which is recognized by laws and regulations, including, but not limited to, HIPAA, the FTC Act, and common law.

176. Defendant was in a superior position to ensure its data security practices were sufficient to protect against the foreseeable risk of harm to Plaintiffs and Class Members from a data breach.

177. Defendant knew that Plaintiffs and Class Members relied on it to protect their Private Information. Plaintiffs and Class Members were not in a position to assess the data security practices used by Defendant. Because they had no means to identify Defendant's security deficiencies, Plaintiffs and Class Members had no opportunity to safeguard their Private Information from cybercriminals. Defendant exercised control over the Private

Information stored on its systems and networks; accordingly, Defendant was best positioned and most capable of preventing the harms caused by the Data Breach.

178. Defendant was aware, or should have been aware, of the fact that cybercriminals routinely target healthcare entities through cyberattacks in an attempt to steal valuable Private Information. In other words, Defendant knew of a foreseeable risk to its data security systems but failed to implement reasonable security measures.

179. Defendant owed Plaintiffs and Class Members a common law duty to use reasonable care to avoid causing foreseeable risk of harm to Plaintiffs and the Class when obtaining, storing, using, and managing their Private Information, including taking action to reasonably safeguard or delete such data and providing notification to Plaintiffs and Class Members of any breach in a timely manner so that appropriate action could be taken to minimize losses.

180. Defendant's duty extended to protecting Plaintiffs and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to such risk, or defeats protections put in place to guard against that risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B.

181. Defendant had a duty to protect and safeguard the Private Information of Plaintiffs and the Class from unauthorized access and disclosure. Additionally, Defendant owed Plaintiffs and the Class a duty:

a. to exercise reasonable care in designing, implementing, maintaining, monitoring, and testing its networks, systems, protocols, policies, procedures and practices to ensure that Plaintiffs' and Class Members' Private Information was adequately secured from impermissible release, disclosure, and publication;

b. to protect Plaintiffs' and Class Members' Private Information by using reasonable and adequate data security practices and procedures;

c. to implement processes to quickly detect a data breach, security incident, or intrusion involving its networks and servers; and

d. to promptly notify Plaintiffs and Class Members of any data breach, security incident, or intrusion that affected or may have affected their Private Information.

182. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Plaintiffs' and Class Members' Private Information.

183. The specific negligent acts and omissions committed by Defendant include, but are not limited to:

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

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

c. Failing to ensure its email systems had plans in place to maintain reasonable data security safeguards;

d. Failing to implement and maintain adequate mitigation policies and procedures;

e. Allowing unauthorized access to Plaintiffs' and Class Members' Private Information;

f. Failing to detect in a timely manner that Plaintiffs' and Class Members' Private Information had been compromised; and

g. Failing to timely notify Plaintiffs and Class Members about the Data Breach so they could take appropriate steps to mitigate the potential for identity theft and other damages.

184. Defendant's willful failure to abide by its duties to Plaintiffs and Class Members was wrongful, reckless, and grossly negligent, considering the foreseeable risks and known threats.

185. It was foreseeable that Defendant's failure to use reasonable measures to protect Plaintiffs' and Class Members' Private Information would result in injury to Plaintiffs and Class Members.

186. Furthermore, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the healthcare industry.

187. As a direct and proximate result of Defendant's negligent conduct, including, but not limited to, its failure to implement and maintain reasonable data security practices

and procedures as described above, Plaintiffs and the Class have suffered damages and are at imminent risk of additional harms and damages (as alleged above).

188. Through Defendant's acts and omissions described herein, including but not limited to Defendant's failure to protect the Private Information of Plaintiffs and Class Members from being stolen and misused, Defendant unlawfully breached its duty to use reasonable care to adequately protect and secure the Private Information of Plaintiffs and Class Members while it was within Defendant's possession and control.

189. Further, through its failure to provide timely and clear notification of the Data Breach to Plaintiffs and Class Members, Defendant prevented Plaintiffs and Class Members from taking meaningful, proactive steps to secure their Private Information and mitigate the impact of the Data Breach.

190. Plaintiffs and Class Members could have taken actions earlier had they been timely notified of the Data Breach.

191. Plaintiffs and Class Members could have enrolled in credit monitoring, instituted credit freezes, and changed their passwords, among other things, had they been alerted to the Data Breach more quickly.

192. Plaintiffs and Class Members suffered harm from Defendant's delay in notifying them of the Data Breach.

193. As a direct and proximate result of Defendant's conduct, including, but not limited to, Defendant's failure to implement and maintain reasonable data security practices and procedures, Plaintiffs and Class Members have suffered or will suffer injury

and damages, including, but not limited to: (i) the loss of the opportunity to determine for themselves how their Private Information is used; (ii) the publication and theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, fraud, and/or unauthorized use of their Private Information, including the need for substantial credit monitoring and identity protection services for an extended period of time; (iv) lost time and opportunity costs associated with efforts expended to address and mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest and recover from fraud and identity theft; (v) costs associated with placing freezes on credit reports and password protections; (vi) anxiety, emotional distress, loss of privacy, and other economic and non-economic losses; (vii) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of compromised Private Information for the rest of their lives. Thus, Plaintiffs and the Class are entitled to damages in an amount to be proven at trial.

194. The damages Plaintiffs and the Class have suffered and will suffer (as alleged above) were and are the direct and proximate result of Defendant's negligent conduct.

195. Plaintiffs and the Class have suffered cognizable injuries and are entitled to actual and punitive damages in an amount to be proven at trial.

SECOND CAUSE OF ACTION
NEGLIGENCE *PER SE*
(On Behalf of Plaintiffs and the Class)

196. Plaintiffs re-allege and incorporate all preceding factual paragraphs as though fully set forth herein.

197. Defendant had a duty to implement and maintain reasonable data security practices pursuant to Section 5 of the FTC Act, 15 U.S.C. § 45(a), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect sensitive and confidential data.

198. 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 PII/PHI. The FTC publications and orders described above also formed part of the basis of Defendant's duty in this regard.

199. Defendant solicited, collected, stored, and maintained Plaintiffs' and Class Members' Private Information as part of its regular business, which affects commerce.

200. Defendant violated the FTC Act by failing to use reasonable measures to protect Plaintiffs' and Class Members' Private Information and by failing to comply with applicable industry standards, as described herein.

201. Defendant breached its duties to Plaintiffs and the Class under the FTC Act by failing to implement and maintain fair, reasonable, and adequate data security practices to safeguard Plaintiffs' and Class Members' Private Information, and by failing to provide prompt notice of the Data Breach without unreasonable delay.

202. Defendant's multiple failures to comply with applicable laws and regulations constitutes negligence *per se*.

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

204. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, like EMSA, that fail to employ reasonable data security measures and avoid unfair and deceptive practices, causing the same harm as that suffered by Plaintiffs and the Class.

205. Defendant breached its duties to Plaintiffs and the Class by unreasonably delaying and failing to provide notice of the Data Breach expeditiously and/or as soon as practicable to Plaintiffs and the Class.

206. Defendant's violations of the FTC Act constitute negligence *per se*.

207. As a direct and proximate result of Defendant's negligence *per se*, Plaintiffs and the Class have suffered, and continue to suffer, damages arising from the Data Breach, as alleged above.

208. The injury and harm that Plaintiffs and Class members suffered (as alleged above) was the direct and proximate result of Defendant's negligence *per se*.

209. Defendant also had a duty to use reasonable security measures under HIPAA, which requires covered entities, including EMSA, to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). Some or all of the medical information at issue in this action constitutes "protected health information" within the meaning of HIPAA.

210. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, *et seq*. These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling Private Information. HHS subsequently promulgated multiple regulations under the authority of the Administrative Simplification provisions of HIPAA. These rules include 45 C.F.R. § 164.304, 45 C.F.R. § 164.306(a)(1-4), 45 C.F.R. § 164.312(a)(1), 45 C.F.R. § 164.308(a)(1)(i), 45 C.F.R. § 164.308(a)(1)(ii)(D), and 45 C.F.R. § 164.530(b).

211. Defendant's violations of HIPAA constitute negligence *per se*.

212. Plaintiffs and the Class are within the class of persons HIPAA was intended to protect.

213. The harm that occurred as a result of the Data Breach is the type of harm HIPAA was intended to guard against.

214. Defendant's duty to use reasonable care in protecting Plaintiffs' and Class Members' Private Information arose not only as a result of the statutes and regulations described above but also because Defendant is bound by industry standards to protect and secure Private Information in its possession and control.

215. As a direct and proximate result of Defendant's negligence *per se*, Plaintiffs and the Class have suffered and will suffer injury, including but not limited to: (i) actual instances of identity theft or fraud; (ii) the compromise, publication, and/or theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, fraud, and/or unauthorized use of their Private Information; (iv) lost time and opportunity costs associated with efforts to mitigate the actual and future consequences of the Data Breach, including, but not limited to, time and resources spent researching how to prevent, detect, contest, and recover from fraud and identity theft; (v) costs associated with placing or removing freezes on credit reports; (vi) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the ongoing impact of the Data Breach for the remainder of the lives of Plaintiffs and the Class.

216. Additionally, as a direct and proximate result of Defendant's negligence *per se*, Plaintiffs and the Class have suffered and will suffer imminent and impending injuries arising from the increased risk of future fraud and identity theft.

217. As a direct and proximate result of Defendant's negligence *per se*, Plaintiffs and the Class are entitled to recover actual, consequential, and nominal damages.

218. Plaintiffs and the Class have suffered injury and are entitled to damages in amounts to be proven at trial.

THIRD CAUSE OF ACTION
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiffs and the Class)

219. Plaintiffs re-allege and incorporate all preceding factual paragraphs as though fully set forth herein.

220. Defendant solicited, collected, stored, and maintained Plaintiffs' and Class Members' Private Information, including their Social Security numbers and other sensitive personal and medical information, as part of Defendant's regular business practices.

221. Plaintiffs and Class Members were required to provide their Private Information to Defendant in order to receive medical services or as a condition of their employment. Plaintiffs and Class Members paid money, or money was paid on their behalf, to Defendant in exchange for medical services and/or employment.

222. Defendant solicited and accepted possession of Plaintiffs' and Class Members' Private Information for the purpose of providing medical services and/or employment to Plaintiffs and Class Members.

223. In delivering, directly or indirectly, their Private Information to Defendant and paying for healthcare services, Plaintiffs and Class Members intended and understood that Defendant would adequately safeguard their Private Information.

224. Plaintiffs and Class Members reasonably expected that the Private Information they entrusted to EMSA, in order to receive medical services or as a condition of their employment, would remain confidential and would not be shared or disclosed to criminal third parties.

225. Plaintiffs and Defendant had a mutual understanding that EMSA would implement and maintain adequate and reasonable data security practices and procedures to protect Plaintiffs' and Class Members' sensitive Private Information. Plaintiffs and Defendant also shared an expectation and understanding that EMSA would not share or disclose, whether intentionally or unintentionally, the sensitive Private Information in its possession and control.

226. Based on Defendant's representations, legal obligations, and acceptance of Plaintiffs' and Class Members' Private Information, Defendant had a duty to safeguard the Private Information in its possession through the use of reasonable data security practices.

227. When Plaintiffs and Class Members paid money and provided their Private Information to EMSA and/or their healthcare providers, either directly or indirectly, in exchange for goods or services, they entered into implied contracts with Defendant.

228. Defendant entered into implied contracts with Plaintiffs and the Class under which Defendant agreed to comply with its statutory and common law duties to safeguard

and protect Plaintiffs' and Class Members' Private Information and to timely notify Plaintiffs and Class Members of a data breach.

229. The implied promise of confidentiality includes consideration beyond those pre-existing duties owed under Section 5 of the FTC Act, HIPAA, and other state and federal regulations. The additional consideration included implied promises to take adequate steps to comply with specific industry data security standards and FTC guidelines on data security.

230. The implied promises include, but are not limited to: (i) taking steps to ensure any agents or vendors who are granted access to Private Information protect the confidentiality of that information; (ii) taking steps to ensure that Private Information in the possession and control of Defendant, its agents, and/or vendors is restricted and limited to achieve an authorized medical purpose; (iii) restricting access to qualified and trained agents and/or vendors; (iv) designing and implementing appropriate retention policies to protect the Private Information from unauthorized access and disclosure; (v) applying or requiring proper encryption of the Private Information; (vi) requiring multifactor authentication for access to the Private Information; and (vii) other steps necessary to protect against foreseeable data breaches.

231. Plaintiffs and Class Members (or their doctors and healthcare providers) would not have entrusted their Private Information to Defendant in the absence of such implied contracts.

232. Defendant recognized that Plaintiffs' and Class Members' Private Information is highly sensitive and must be protected, and that this protection was of material importance to Plaintiffs and Class Members.

233. Had Defendant disclosed to Plaintiffs and Class Members (or their doctors and healthcare providers) that it did not have adequate data security practices to secure their Private Information, Plaintiffs and Class Members (or their doctors and healthcare providers) would not have provided their Private Information to Defendant.

234. Plaintiffs and Class Members (or their doctors and healthcare providers) fully performed their obligations under the implied contracts with Defendant.

235. Defendant breached the implied contracts with Plaintiffs and Class Members by failing to safeguard Plaintiffs' and Class Members' Private Information and by failing to provide them with timely and accurate notice of the Data Breach.

236. As a direct and proximate result of Defendant's breach of the implied contracts, Plaintiffs and Class Members have suffered damages, including foreseeable consequential damages that Defendant knew about when it solicited and collected Plaintiffs' and Class Members' Private Information.

237. Alternatively, Plaintiffs and Class Members were the intended beneficiaries of data protection agreements entered into between Defendant and healthcare providers.

238. Plaintiffs and the Class have suffered injuries as described herein, and are entitled to actual and punitive damages, statutory damages, and reasonable attorneys' fees and costs, in an amount to be proven at trial.

FOURTH CAUSE OF ACTION
UNJUST ENRICHMENT
(On Behalf of Plaintiffs and the Class)

239. Plaintiffs re-allege and incorporate all preceding factual paragraphs as though fully set forth herein.

240. Plaintiffs allege this claim in the alternative to their breach of implied contract claim.

241. Plaintiffs and the Class provided their Private Information to EMSA in order to receive medical services and/or as a condition of their employment.

242. By conferring their Private Information to Defendant, Plaintiffs and Class Members reasonably understood Defendant would be responsible for securing their Private Information from unauthorized access and disclosure.

243. Upon information and belief, Defendant funds its data security measures entirely from its general revenue, including from money it makes based on protecting Plaintiffs' and Class Members' Private Information.

244. Plaintiffs and Class Members paid Defendant and/or their healthcare providers a certain sum of money, which was used to fund data security via contracts with Defendant.

245. As such, a portion of the payments made by or on behalf of Plaintiffs and the Class was to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendant.

246. There is a direct nexus between money paid to Defendant and the

requirement that Defendant keep Plaintiffs' and Class Members' Private Information confidential and protected from unauthorized access and disclosure.

247. Protecting the Private Information of Plaintiffs and Class Members is integral to Defendant's business. Without their Private Information, Defendant would be unable to provide services comprising Defendant's core business.

248. Plaintiffs' and Class Members' Private Information has monetary value.

249. Plaintiffs and Class Members directly and indirectly conferred a monetary benefit on Defendant. They indirectly conferred a monetary benefit on Defendant by purchasing goods and/or services from entities that contracted with Defendant, and from which Defendant received compensation to protect certain data. Plaintiffs and Class Members directly conferred a monetary benefit on Defendant by supplying their Private Information, from which Defendant derives its business, and which should have been protected with adequate data security.

250. Defendant solicited, collected, stored, and maintained Plaintiffs' and Class Members' Private Information, and as such, Defendant had direct knowledge of the monetary benefits conferred upon it by Plaintiffs and the Class. Defendant profited from these transactions and used Plaintiffs' and Class Members' Private Information for business purposes.

251. Indeed, Plaintiffs and Class Members who were patients of EMSA provided monetary payment to EMSA and therefore conferred a benefit unto EMSA.

252. Defendant appreciated that a monetary benefit was being conferred upon it

by Plaintiffs and Class Members and accepted that monetary benefit.

253. Under the facts and circumstances outlined above, however, it is inequitable for Defendant to retain that benefit without payment of the value thereof.

254. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' Private Information.

255. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to increase its own profits 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 decision to prioritize its own profits over the requisite data security.

256. Under the principles of equity and good conscience, Defendant should not be permitted to retain the monetary benefit belonging to Plaintiffs and Class Members, because Defendant failed to implement appropriate data management and security measures.

257. Defendant acquired Plaintiffs' and Class Members' Private Information through inequitable means in that it failed to disclose its inadequate data security practices, as previously alleged.

258. If Plaintiffs and Class Members knew that Defendant had not secured their Private Information, they would not have allowed Defendant to collect their Private Information.

259. Plaintiffs and Class Members have no adequate remedy at law.

260. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered or will suffer injury, including, but not limited to: (i) actual identity theft and fraud; (ii) loss of the opportunity to control how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, fraud, and/or unauthorized use of their Private Information; (v) lost time and opportunity costs associated with efforts to mitigate the actual and future consequences of the Data Breach, including, but not limited to, effort and time spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in their continued possession; and/or (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

261. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

262. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, all gains that they unjustly received.

FIFTH CAUSE OF ACTION
BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiffs and the Class)

263. Plaintiffs re-allege and incorporate all preceding factual paragraphs as though fully set forth herein.

264. In light of the special relationship between EMSA, as a medical provider and/or employer, and Plaintiffs and Class Members, Defendant became a fiduciary by undertaking a guardianship of Plaintiffs' and Class Members' Private Information.

265. A physician has a fiduciary duty to not disclose a patient's medical information.

266. Defendant had a fiduciary duty, created by its undertaking and guardianship of Plaintiffs' and the Class Members' Private Information, to act primarily for the benefit of Plaintiffs and Class Members.

267. This duty included the obligation and responsibility to:

a. safeguard Plaintiffs' and Class Members' Private Information;

b. timely detect and notify Plaintiffs and the Class in the event of a data breach;

c. only utilize vendors with adequate data security infrastructure, procedures, and protocols;

d. establish and implement appropriate oversight and monitoring procedures for the activities of its vendors.

268. In order to provide Plaintiffs and Class Members with medical services,

Defendant required that Plaintiffs and Class Members provide their Private Information to EMSA.

269. Defendant knowingly undertook the responsibility and duties related to the possession of Plaintiffs' and Class Members' Private Information, for the benefit of Plaintiffs and Class Members and in order to provide Plaintiffs and Class Members with medical services.

270. Defendant had a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of its relationship with them.

271. Defendant breached the fiduciary duties it owed to Plaintiffs and Class Members by failing to protect Plaintiffs' and Class Members' Private Information.

272. Defendant further breached the fiduciary duties it owed to Plaintiffs and Class Members by failing to timely notify and/or warn Plaintiffs and Class Members of the Data Breach and by utilizing a vendor with inadequate data security infrastructure, procedures, and protocols.

273. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiffs and Class Members have suffered or will suffer concrete injury, including, but not limited to: (i) actual misuse of their Private Information in the form of identity theft and fraud; (ii) the loss of the opportunity to control how their Private Information is used; (iii) the unauthorized access, acquisition, appropriation, disclosure, encumbrance, exfiltration, release, theft, use, and/or viewing of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft,

fraud, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with efforts to mitigate the actual and future consequences of the Data Breach, including, but not limited to, time and effort spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

274. 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 other forms of injury and/or harm, and other economic and non-economic losses.

SIXTH CAUSE OF ACTION
DECLARATORY AND INJUNCTIVE RELIEF
(On Behalf of Plaintiffs and the Class)

275. Plaintiffs re-allege and incorporate all preceding factual paragraphs as though fully set forth herein.

276. As previously alleged, Plaintiffs and members of the Class entered into implied contracts with Defendant, which contracts required Defendant to provide adequate security for the protection of the Private Information Defendant collected from Plaintiffs and the Class.

277. Defendant owed and still owes a duty of care to Plaintiffs and Class Members that requires it to adequately secure Plaintiffs' and Class Members' Private Information.

278. Upon information and belief, Defendant still possesses Plaintiffs' and Class Members' Private Information.

279. Defendant has not satisfied its contractual obligations and legal duties to Plaintiffs and Class Members.

280. Since the Data Breach, Defendant has not announced any changes to its data security infrastructure, processes or procedures to fix the vulnerabilities in its computer systems and/or security practices which permitted the Data Breach to occur and go undetected and, thereby, prevent further attacks.

281. Defendant has not satisfied its contractual obligations and legal duties to Plaintiffs and the Class. In fact, now that Defendant's insufficient data security is known to hackers, the Private Information in Defendant's possession is even more vulnerable to cyberattacks.

282. Further, Plaintiffs and Class Members are at risk of additional or further harm due to the exposure of their Private Information and Defendant's failure to address the security failings that led to such exposure.

283. There is no reason to believe that Defendant's security measures are any more adequate now than they were before the Data Breach.

284. Plaintiffs and the Class, therefore, seek a declaration (1) that Defendant's existing security measures do not comply with its contractual obligations and duties of care

to provide adequate security, and (2) that to comply with its contractual obligations and duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to:

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

b. Ordering that Defendant engage third-party security auditors and internal personnel to run automated security monitoring;

c. Ordering that Defendant audit, test, and train its security personnel regarding any new or modified procedures;

d. Ordering that Defendant segment employee and patient data by, among other things, creating firewalls and access controls so that if one area of Defendant's systems is compromised, hackers cannot gain access to other portions of Defendant's systems;

e. Ordering that Defendant purge, delete, and destroy, in a reasonably secure manner, customer data not necessary for their provisions of services;

f. Ordering that Defendant conduct regular database scanning and security checks; and

g. Ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiffs and the Class pray for judgment against Defendant as follows:

a. For an order certifying this action as a Class Action under 12 O.S. § 2023, defining the Class as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiffs are proper representatives of the Class requested herein;

b. For a judgment in favor of Plaintiffs and the Class, awarding them appropriate monetary relief, including compensatory damages, punitive damages, nominal damages, attorneys' fees, expenses, costs, and such other and further relief as is just and proper;

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

d. For an order requiring Defendant to pay the costs involved in notifying the Class about the judgment and administering the claims process;

e. For a judgment in favor of Plaintiffs and the Class, awarding them pre-judgment and post-judgment interest, reasonable attorneys' fees, costs, and expenses as allowable by law; and

f. For an award of such other and further relief as this Court may deem just and proper.

VIII. DEMAND FOR JURY TRIAL

Plaintiffs hereby demand a trial by jury on any and all issues raised in this Consolidated Class Action Petition so triable as of right.

Dated: July 10, 2024

Respectfully submitted,

/s/ William B. Federman

William B. Federman, OBA #2853
Kennedy M. Brian, OBA #34617
FEDERMAN & SHERWOOD
10205 North Pennsylvania Avenue
Oklahoma City, OK 73120
T: (405) 235-1560
E: wbf@federmanlaw.com
E: kpb@federmanlaw.com

Interim Lead Counsel for Plaintiffs and the Class

CERTIFICATE OF SERVICE

I, the undersigned, hereby certify that on July 10, 2024, a true and correct copy of the foregoing was mailed via first class mail to the following:

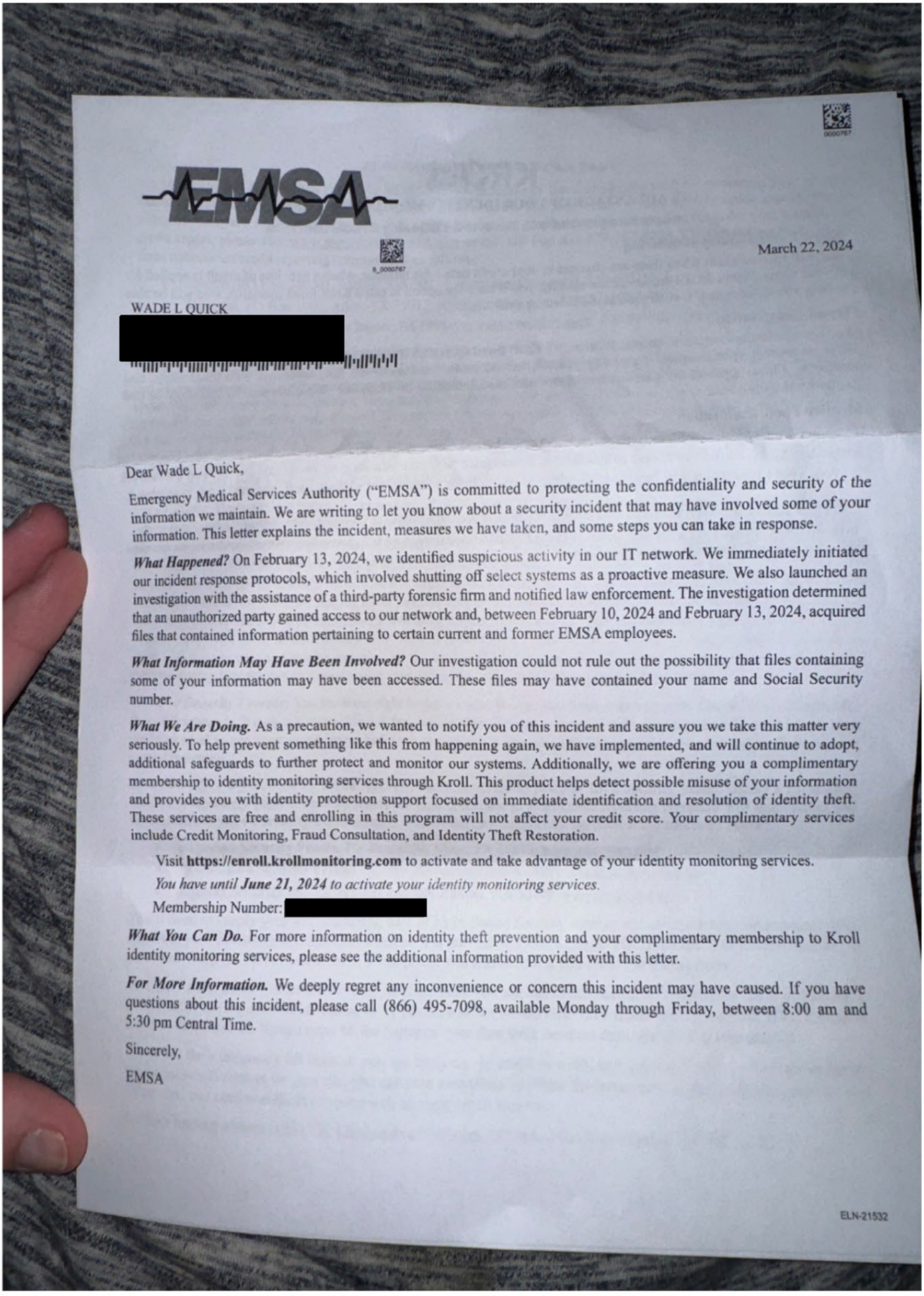
Kristopher E. Koepsel
RIGSS ABNEY NEAL TURPEN
ORBISON & LEWIS PC
502 West 6th Street
Tulsa, OK 74119
E: kkoepsel@riggsabney.com

John P. Hutchins
Olivia S. William
BAKER HOSTETLER LLP
1170 Peachtree Street, NE, Suite 24000
Atlanta, GA 30309
E: jhutchins@bakerlaw.com
E: owilliams@bakerlaw.com

Counsel for Defendant

/s/ William B. Federman
William B. Federman, OBA #2853

EXHIBIT 1



EMSA

March 22, 2024

WADE L QUICK
[redacted]

Dear Wade L Quick,

Emergency Medical Services Authority ("EMSA") is committed to protecting the confidentiality and security of the information we maintain. We are writing to let you know about a security incident that may have involved some of your information. This letter explains the incident, measures we have taken, and some steps you can take in response.

What Happened? On February 13, 2024, we identified suspicious activity in our IT network. We immediately initiated our incident response protocols, which involved shutting off select systems as a proactive measure. We also launched an investigation with the assistance of a third-party forensic firm and notified law enforcement. The investigation determined that an unauthorized party gained access to our network and, between February 10, 2024 and February 13, 2024, acquired files that contained information pertaining to certain current and former EMSA employees.

What Information May Have Been Involved? Our investigation could not rule out the possibility that files containing some of your information may have been accessed. These files may have contained your name and Social Security number.

What We Are Doing. As a precaution, we wanted to notify you of this incident and assure you we take this matter very seriously. To help prevent something like this from happening again, we have implemented, and will continue to adopt, additional safeguards to further protect and monitor our systems. Additionally, we are offering you a complimentary membership to identity monitoring services through Kroll. This product helps detect possible misuse of your information and provides you with identity protection support focused on immediate identification and resolution of identity theft. These services are free and enrolling in this program will not affect your credit score. Your complimentary services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit **https://enroll.krollmonitoring.com** to activate and take advantage of your identity monitoring services.

*You have until **June 21, 2024** to activate your identity monitoring services.*

Membership Number: [redacted]

What You Can Do. For more information on identity theft prevention and your complimentary membership to Kroll identity monitoring services, please see the additional information provided with this letter.

For More Information. We deeply regret any inconvenience or concern this incident may have caused. If you have questions about this incident, please call (866) 495-7098, available Monday through Friday, between 8:00 am and 5:30 pm Central Time.

Sincerely,

EMSA

ELN-21532

EXHIBIT 2

EMSA

[redacted]

April 16, 2024

LAURA LANCE
[redacted]

Dear Laura Lance,

Emergency Medical Services Authority ("EMSA") is committed to protecting the confidentiality and security of the information we maintain. EMSA is an ambulance services provider serving communities throughout central and eastern Oklahoma. We are writing to let you know about a security incident that may have involved some of your information. This letter explains the incident, measures we have taken, and some steps you can take in response.

What Happened? On February 13, 2024, we identified suspicious activity in our IT network. We immediately initiated our incident response protocols, which involved shutting off select systems as a proactive measure. We also launched an investigation with the assistance of a third-party forensic firm and notified law enforcement. The investigation determined that an unauthorized party gained access to our network and, between February 10, 2024 and February 13, 2024, acquired files that contained information pertaining to certain EMSA patients.

What Information May Have Been Involved? Our investigation determined that files containing some of your information were accessed and/or acquired. These files contained one or more of the following: your name, address, date of birth, Social Security number, date of service, and/or name of primary care provider.

What We Are Doing. As a precaution, we wanted to notify you of this incident and assure you we take this matter very seriously. To help prevent something like this from happening again, we have implemented, and will continue to adopt, additional safeguards to further protect and monitor our systems. Additionally, we are offering you a complimentary membership to identity monitoring services through Kroll. This product helps detect possible misuse of your information and provides you with identity protection support focused on immediate identification and resolution of identity theft. These services are free and enrolling in this program will not affect your credit score. Your complimentary services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit **https://enroll.krollmonitoring.com** to activate and take advantage of your identity monitoring services.
*You have until **July 5, 2024** to activate your identity monitoring services.*
Membership Number: [redacted]

What You Can Do. For more information on identity theft prevention and your complimentary membership to Kroll identity monitoring services, please see the additional information provided with this letter.

For More Information. We deeply regret any inconvenience or concern this incident may have caused. If you have questions about this incident, please call (866) 495-7098, available Monday through Friday, between 8:00 am and 5:30 pm Central Time.

Sincerely,

EMSA