UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

HERMAN SAUNDERS, individually and on behalf of all others similarly situated, Plaintiff, v. EMPRESS AMBULANCE SERVICE LLC d/b/a EMPRESS EMS, Defendant.	Case No. **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Herman Saunders ("Plaintiff"), individually and on behalf of all other similarly situated individuals (the "Class Members," as defined below), by and through the undersigned counsel, file this Class Action Complaint against Empress Ambulance Service, LLC d/b/a Empress EMS. ("Empress EMS" or "Defendant") and allege the following based on personal knowledge of facts and on information and belief based on the investigation of counsel as to all other matters.

I. NATURE OF THE ACTION

1. Empress EMS, an emergency medical services and aftercare transportation provider.

2. Plaintiff and the Class Members (as further defined below) are individuals who entrusted Defendant with their personally identifiable information ("PII"). Defendant betrayed Plaintiff's trust and that of the other Class Members by failing to properly safeguard and protect their PII and thereby enabling cybercriminals to steal their PII.

3. This class action seeks to redress Empress EMS's unlawful, willful and wanton failure to protect the PII of 318,558 individuals that was disclosed in a major data breach that was discovered in July 2022 (the "Data Breach" or "Breach"), in violation of its legal obligations.

4. The Data Breach occurred as a result of unauthorized third-party actors who were able to infiltrate Defendant's inadequately secured system and gain access to Defendant's network on May 26, 2022. Defendant did not detect this unauthorized access until July 14, 2022 – but at that point, nearly two months had passed since this unauthorized access had initially occurred and, in that time, the hackers had unfettered access to Defendant's network. Thus, the hackers "copied a small subset of files on July 13, 2022" according to Defendant's Notice of Data Breach (the "Notice").

5. The PII accessed or even copied by cybercriminals included individuals' names, dates of service, Social Security numbers, and insurance information.

6. Due to Defendant's negligence, cyber criminals obtained everything they need to commit identity theft and wreak havoc on the financial and personal lives of thousands of individuals.

7. For the rest of their lives, Plaintiff and the Class Members will have to deal with the danger of identity thieves possessing their PII. Even those Class Members who have yet to experience identity theft have to spend time responding to the Breach and are at an immediate and heightened risk of all manners of identity theft as a direct and proximate result of the Data Breach. Plaintiff and Class Members have incurred, and will continue to incur, damages in the form of, among other things, identity theft, attempted identity theft, lost time and expenses mitigating harms, increased risk of harm, damaged credit, diminished value of PII, loss of privacy, and/or additional damages as described below.

8. Plaintiff brings this action individually and on behalf of the Class, seeking compensatory damages, punitive damages, restitution, and injunctive and declaratory relief, reasonable attorney fees and costs, and all other remedies this Court deems proper.

II. THE PARTIES

Plaintiff

9. Plaintiff is domiciled in and a citizen of New York. Plaintiff received notification from Defendant that his information, including Social Security number, was exposed in the Data Breach.

Defendant Empress EMS

10. Defendant Empress Ambulance Services LLC d/b/a Empress EMS is a Delaware corporation with its principal place of business located in Yonkers, New York.

III. JURISDICTION AND VENUE

11. This Court has diversity jurisdiction over this action under the Class Action Fairness Act (CAFA), 28 U.S.C. § 1332(d), because this is a class action involving more than 100 class members, the amount in controversy exceeds $5,000,000, exclusive of interest and costs, and many members of the class are citizens of states different from Defendant.

12. This Court has personal jurisdiction over Defendant because its principal place of business is in this State, it regularly transacts business in this District.

13. Venue is likewise proper as to Defendant in this District because a substantial part of the events or omissions giving rise to the claim occurred in this District. 28 U.S.C. § 1391(b)(2).

IV. FACTUAL ALLEGATIONS

A. The Data Breach

14. On July 14, 2022, Empress EMS noticed suspicious activity on this network. Specifically, Defendant noticed that files in certain systems had been encrypted as part of a ransomware attack.[1] A subsequent forensic investigation determined that the unauthorized third-party actors had actually gained access to Defendant's network on May 26, 2022.[2] Defendant did not detect this unauthorized access until July 14, 2022. Thus, cybercriminals had undetected and unfettered access to Defendant's network for nearly two months. During that time, the unauthorized cybercriminals acquired hundreds of thousands of people's most sensitive PII.[3]

15. According to databreaches.net, a data breach reporting website, the cyberattack on Defendant was conducted by a ransomware hacking group called, Hive.[4] Based on emails from Hive that were shared with databreaches.net,[5] the cybercriminals had communications with Empress EMS following the breach, including the below:

> ! ! ! DO NOT TRY TO DECRYPT OR CHANGE ENCRYPTED FILES ON YOUR COMPUTERS, IT WILL COMPLETELY DESTROY THEM ! ! !
>
> Ladies and gentlemen! Attention, please!
> This is HIVE ransomware team.
>
> We infiltrated your network and stayed there for 12 days (it was enough to study all your documentation and gain access to your files and services), encrypted your servers.
> Downloaded most important information with a total size over 280 GB

[1] *See* https://www.hipaajournal.com/new-york-ambulance-service-discloses-ransomware-attack-and-318k-record-data-breach/.

[2] *Id.*

[3] *Id.*

[4] https://www.databreaches.net/ny-empress-ems-hit-by-hive-ransomware/.

[5] *Id.*

> Few details about information we have downloaded:
> – contracts, nda and other agreements documents
> – company private info (budgets, plans, investments, company bank statements, etc.)
> – employees info (SSN numbers, emails, addresses, passports, phone numbers, payments, working hours, etc.)
> – customers info (SSN numbers, emails, addresses, passports, phone numbers, payments, working hours, etc.)
> – SQL databases with reports, business data, customers data, etc.
> – approximate number of personal records including addresses and ssn's data is above 10000 units

16. Accordingly, it is evident that the cybercriminals accessed and downloaded highly sensitive and valuable information, including the PII of Plaintiff and the Class.

17. Empress EMS was grossly negligent and disregarded the obvious and substantial risks of such an attack—an attack that was undetected for weeks and that was only detected after the cybercriminals chose to make their presence on Defendant's system known.

18. Empress EMS failed to take the necessary precautions required to safeguard and protect Plaintiff's and the other Class Members' PII from unauthorized disclosure. Defendant's actions represent a flagrant disregard of its patients' rights, both as to privacy and property.

B. Plaintiff's Experience

19. In order to receive needed medical services, Plaintiff was required to provide Empress EMS with his PII, including the information compromised in the Data Breach.

20. In or around September 2022, Plaintiff received a breach notification letter from Empress EMS informing him that his personal information, including name, Social Security Number, and insurance information were stolen in the Data Breach—this was *two months* after the Data Breach was identified by Defendant.

21. Plaintiff has spent numerous hours responding to the Data Breach and the identity theft that has occurred because of it. Among other things, Plaintiff has spent time researching the facts of the Data Breach, confirming the veracity of the Notice he received, monitoring his accounts and personal information, and taking other steps in an attempt to mitigate the harms caused as a result of the Data Breach.

22. Plaintiff has been careful to protect and monitor his identity and personal information.

23. To his knowledge, Plaintiff has not been the victim of any other data breach.

C. Cyber Criminals Have Used and Will Continue to Use Plaintiff's PII to Defraud Them

24. PII is of great value to hackers and cyber criminals, and the data stolen in the Data Breach can and will be used in a variety sordid ways for criminals to exploit Plaintiff and the Class Members and to profit off their misfortune.

25. Each year, identity theft causes tens of billions of dollars of losses to victims in the United States.[6] For example, with the PII stolen in the Data Breach, including Social Security numbers, identity thieves can open financial accounts, apply for credit, 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.[7] These criminal

[6] "Facts + Statistics: Identity Theft and Cybercrime," Insurance Info. Inst., https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (discussing Javelin Strategy & Research's report "2018 Identity Fraud: Fraud Enters a New Era of Complexity").

[7] *See, e.g.*, Christine DiGangi, *5 Ways an Identity Thief Can Use Your Social Security Number*, Nov. 2, 2017, https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/.

activities have and will result in devastating financial and personal losses to Plaintiff and the Class Members.

26. 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.[8]
>
> [Emphasis added.]

27. PII is such a valuable commodity to identity thieves that once it has been compromised, criminals will use it for years.[9]

28. This was a financially motivated Breach, as the reason the cyber criminals go through the trouble of running a targeted ransomware campaign against companies like Empress EMS is to get information that they can monetize by selling on the black market for use in the kinds of criminal activity described herein. Indeed, a social security number, date of birth, and full name can sell for $60 to $80 on the digital black market.[10] "[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."[11]

---

[8] *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/.

[9] *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/assets/270/262904.htmlu.

[10] Michael Kan, *Here's How Much Your Identity Goes for on the Dark Web*, Nov. 15, 2017, https://www.pcmag.com/news/heres-how-much-your-identity-goes-for-on-the-dark-web.

[11] *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/.

29. These risks are both certainly impending and substantial. As the Federal Trade Commission ("FTC") has reported, if hackers get access to PII, they ***will*** use it.[12]

30. 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.[13]

31. For instance, with a stolen social security number, which is part of the PII compromised in the Data Breach, someone can open financial accounts, get medical care, file fraudulent tax returns, commit crimes, and steal benefits.[14]

32. 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.[15]

33. While some harm has begun already, the full scope of the harm has yet to be realized. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. Once the twelve-months have expired, Plaintiff and Class Members will need to pay for their own identity theft protection and credit monitoring for the rest of their lives due to Empress EMS's gross negligence. Furthermore, identity monitoring

---

[12] Ari Lazarus, *How fast will identity thieves use stolen info?*, FED. TRADE COMM'N (May 24, 2017), https://www.consumer.ftc.gov/blog/2017/05/how-fast-will-identity-thieves-use-stolen-info.

[13] *Data Breaches Are Frequent*, *supra* note 11.

[14] *See, e.g.*, Christine DiGangi, *5 Ways an Identity Thief Can Use Your Social Security Number*, Nov. 2, 2017, https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/.

[15] "Guide for Assisting Identity Theft Victims," Federal Trade Commission, 4 (Sept. 2013), http://www.consumer.ftc.gov/articles/pdf-0119-guide-assisting-id-theft-victims.pdf.

only alerts someone to the fact that they have *already been the victim of identity theft* (*i.e.*, fraudulent acquisition and use of another person's PII)—it does not prevent identity theft.[16] Nor can an identity monitoring service remove personal information from the dark web.[17] "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."[18]

34. As a direct and proximate result of the Data Breach, Plaintiff and the Class have suffered actual identity theft, have been damaged, and have been placed at an imminent, immediate, and continuing increased risk of harm from continued fraud and identity theft. Plaintiff 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 and credit reports for unauthorized activity for years to come. Even more seriously is the identity restoration that individuals must go through, which can include spending countless hours filing police reports, filling out IRS forms, Federal Trade Commission checklists, Department of Motor Vehicle driver's license replacement applications, and calling financial institutions to cancel fraudulent credit applications, to name just a few of the steps Plaintiff and the Class must take.

---

[16] *See, e.g.*, Kayleigh Kulp, *Credit Monitoring Services May Not Be Worth the Cost*, Nov. 30, 2017, https://www.cnbc.com/2017/11/29/credit-monitoring-services-may-not-be-worth-the-cost.html.

[17] *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/.

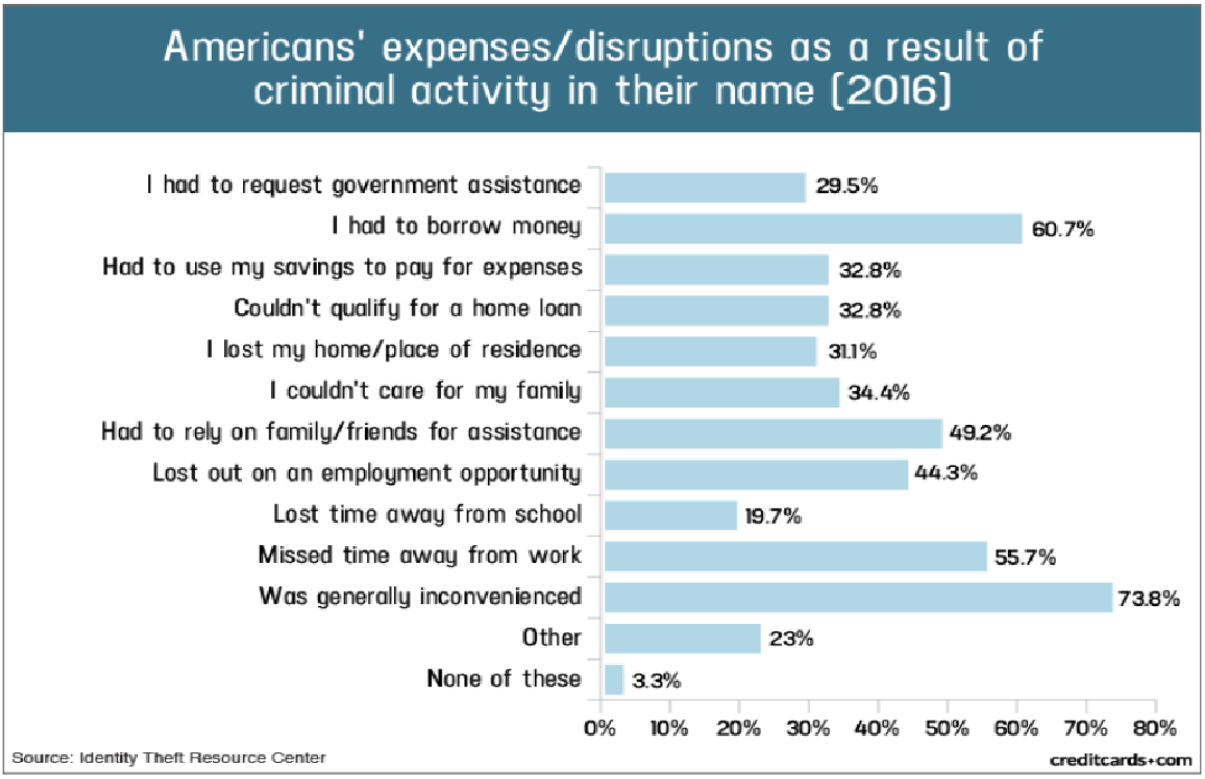
[18] *Id.*

35. Plaintiff and the Class have suffered, and continue to suffer, actual harms for which they are entitled to compensation, including:

a. Actual identity theft, including fraudulent credit inquiries and cards being opened in their names;
b. Trespass, damage to, and theft of their personal property including PII;
c. Improper disclosure of their PII;
d. The imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII being placed in the hands of criminals and having been already misused;
e. Damages flowing from Defendant's untimely and inadequate notification of the data breach, including the uncertainty of whether they need to replace their driver's licenses;
f. Loss of privacy suffered as a result of the Data Breach, including the harm of knowing cyber criminals have their PII and that identity thieves have already used that information to defraud other victims of the Data Breach;
g. Ascertainable losses in the form of time taken to respond to identity theft and attempt to restore identity, including lost opportunities and lost wages from uncompensated time off from work;
h. 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;
i. Ascertainable losses in the form of deprivation of the value of Plaintiff's and Class members' personal information for which there is a well-established and quantifiable national and international market;
j. The loss of use of and access to their credit, accounts, and/or funds;
k. Damage to their credit due to fraudulent use of their PII; and

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

36. Below is a chart that shows the kinds of expenses and disruptions that victims of identity theft experience[19]:



37. Moreover, Plaintiff and Class Members have an interest in ensuring that their information, which remains in the possession of Defendant, is protected from further breaches by the implementation of industry standard security measures and safeguards. Defendant has shown itself wholly incapable of protecting Plaintiff's PII.

38. Defendant itself acknowledged the harm caused by the Data Breach because it offered Plaintiff and Class Members the woefully inadequate twelve months of identity theft repair

[19] Jason Steele, *Credit Card and ID Theft Statistics*, CREDITCARDS.COM (Oct. 24, 2017), https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php.

and monitoring services. Twelve months of identity theft and repair and monitoring is, however, inadequate to protect Plaintiff and Class Members from a lifetime of identity theft risk.

39. At Empress EMS's suggestion, Plaintiff is desperately trying to mitigate the damage that Empress EMS has caused them. Given the kind of PII Empress EMS made accessible to hackers, however, Plaintiff is certain to incur additional damages. Some may even need to go through the long and arduous process of getting a new Social Security number, with all the loss of credit and employment difficulties that come with a new number.[20]

40. None of this should have happened.

D. Defendant was Aware of the Risk of Cyber-Attacks

41. Data security breaches have dominated the headlines for the last two decades. And it doesn't take an IT industry expert to know it. The general public can tell you the names of some of the biggest data breaches: Target,[21] Yahoo,[22] Marriott International,[23] Chipotle, Chili's, Arby's,[24] and others.[25]

[20] *Will a New Social Security Number Affect Your Credit?*, LEXINGTON LAW (Nov. 16, 2015), https://www.lexingtonlaw.com/blog/credit-101/will-a-new-social-security-number-affect-your-credit.html.

[21] Michael Kassner, *Anatomy of the Target Data Breach: Missed Opportunities and Lessons Learned*, ZDNET (Feb. 2, 2015), https://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned/.

[22] Martyn Williams, *Inside the Russian Hack of Yahoo: How They Did It*, CSOONLINE.COM (Oct. 4, 2017), https://www.csoonline.com/article/3180762/inside-the-russian-hack-of-yahoo-how-they-did-it.html.

[23] Patrick Nohe, *The Marriot Data Breach: Full Autopsy*, THE SSL STORE: HASHEDOUT (Mar. 22, 2019), https://www.thesslstore.com/blog/autopsying-the-marriott-data-breach-this-is-why-insurance-matters/.

[24] Alfred Ng, *FBI Nabs Alleged Hackers in Theft of 15M Credit Cards from Chipotle, Others*, CNET (Aug. 1, 2018), https://www.cnet.com/news/fbi-nabs-alleged-hackers-in-theft-of-15m-credit-cards-from-chipotle-others/?ftag=CMG-01-10aaa1b.

[25] *See, e.g.*, Taylor Armerding, *The 18 Biggest Data Breaches of the 21st Century*, CSO ONLINE (Dec. 20, 2018), https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html.

42. As one of medical service provider, Empress EMS should certainly have been aware, and indeed was aware, that it was at risk for a data breach that could expose the PII that it collected and maintained.

43. Indeed, cyberattacks against the healthcare industry have been common for over ten years with the FBI warning as early as 2011 that cybercriminals were "advancing their abilities to attack a system remotely" and "[o]nce a system is compromised, cyber criminals will use their accesses to obtain PII." The FBI further warned that that "the increasing sophistication of cyber criminals will no doubt lead to an escalation in cybercrime."[26]

44. Cyberattacks have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals… because they often have lesser IT defenses and a high incentive to regain access to their data quickly.[27]

45. In fact, according to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in the past year.[28]

46. Defendant was on notice that the FBI has recently been concerned about data security in the healthcare industry. In August 2014, after a cyberattack on Community Health Systems, Inc., the FBI warned companies within the healthcare industry that hackers were

[26] Gordon M. Snow, *Statement before the House Financial Services Committee, Subcommittee on Financial Institutions and Consumer Credit*, FBI (Sept. 14, 2011), https://archives.fbi.gov/archives/news/testimony/cyber-security-threats-to-the-financial-sector.

[27] *FBI, Secret Service Warn of Targeted*, Law360 (Nov. 18, 2019), https://www.law360. arn-of-targeted-ransomware (last visited July 2, 2021).

[28] *See* Maria Henriquez, *Iowa City Hospital Suffers Phishing Attack*, *Security Magazine* (Nov. 23, 2020), https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing-attack

targeting them. The warning stated that "[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining the Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII)."[29]

47. The United States Department of Health and Human Services' Office for Civil Rights urges the use of encryption of data containing sensitive personal information. As long ago as 2014, the Department fined two healthcare companies approximately two million dollars for failing to encrypt laptops containing sensitive personal information. In announcing the fines, Susan McAndrew, the DHHS's Office of Human Rights' deputy director of health information privacy, stated "[o]ur message to these organizations is simple: encryption is your best defense against these incidents."[30]

E. Empress EMS Could Have Prevented the Data Breach

48. Data breaches are preventable.[31] As Lucy Thompson wrote in the DATA BREACH AND ENCRYPTION HANDBOOK, "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."[32] She added that "[o]rganizations that collect, use, store, and share sensitive

[29] Jim Finkle, *FBI Warns Healthcare Firms that they are Targeted by Hackers*, REUTERS (Aug. 2014), https://www.reuters.com/article/us-cybersecurity-healthcare-fbi/fbi-warns-healthcare-firms-they-are-targeted-by-hackers-idUSKBN0GK24U20140820.

[30] "Stolen Laptops Lead to Important HIPAA Settlements," U.S. Dep't of Health and Human Services (Apr. 22, 2014), available at https://wayback.archive-it.org/3926/20170127085330/https://www.hhs.gov/about/news/2014/04/22/stolen-laptops-lead-to-important-hipaa-settlements.html.

[31] Lucy L. Thomson, "Despite the Alarming Trends, Data Breaches Are Preventable," *in* DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012).

[32] *Id.* at 17.

personal data must accept responsibility for protecting the information and ensuring that it is not compromised . . . ."[33]

49. "Most of the 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*."[34]

50. In a Data Breach like this, many failures laid the groundwork for the Breach.

51. The FTC has published guidelines that establish reasonable data security practices for businesses. 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.[35] The 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. The guidelines also recommended 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.

52. Upon information and belief, Empress EMS failed to maintain many reasonable and necessary industry standards necessary to prevent a data breach, including the FTC's

[33] *Id.* at 28.

[34] *Id.*

[35] FTC, *Protecting Personal Information: A Guide for Business*, https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

guidelines. Upon information and belief, Empress EMS 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 reasonable cybersecurity readiness.

53. Among other things, Empress EMS's protection software and endpoint detection were not sufficient to recognize, block, or detect the attack.

54. Empress EMS further had far too much confidential unencrypted information held on its systems.[36]

55. Moreover, it is well-established industry standard practice for a business to dispose of confidential PII once it is no longer needed. The FTC, among others, has repeatedly emphasized the importance of disposing unnecessary PII, saying simply: "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."[37] Empress EMS, rather than following this basic standard of care, kept hundreds of thousands of former patients' unencrypted PII on its network. This greatly expanded the number of victims harmed in the Breach.

F. Empress EMS's Response to the Data Breach is Inadequate to Protect Plaintiff and the Class

56. Empress EMS failed to inform Plaintiff and Class Members of the Data Breach in time for them to protect themselves from identity theft.

---

[36] *See, e.g.*, Adnan Raja, *How to Safeguard Your Business Data with Encryption*, Aug. 14, 2018, https://digitalguardian.com/blog/how-safeguard-your-business-data-encryption.

[37] FTC, *Protecting Personal Information: A Guide for Business*, https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf at p. 6.

57. Empress EMS stated that it discovered the Data Breach in July 2022. However, Empress EMS did not start notifying affected individuals until September 2022. Even then, provide only vague information and not disclose the timeframe in which cybercriminals had been present on Defendant's network, leaving Plaintiff and Class Members unsure as to the scope of information that was compromised and the risks they face.

58. If Empress EMS had detected the Data Breach, investigated it more diligently and reported it sooner, the damages to Plaintiff and the Class could have been mitigated.

V. CLASS ACTION ALLEGATIONS

59. Plaintiff incorporates by reference all preceding paragraphs as if fully restated here.

60. Plaintiff brings this action against Empress EMS on behalf of himself and all other individuals similarly situated under Federal Rule of Civil Procedure 23. Plaintiff asserts all claims on behalf of a nationwide class (the "Class") defined as follows:

> All persons whose personally identifiable information was compromised as a result of the Data Breach, including those who received notification letters from Empress EMS.

61. 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 judicial staff.

62. Plaintiff reserves the right to amend the above definition or to propose subclasses in subsequent pleadings and motions for class certification.

63. The proposed Class meets the requirements of Fed. R. Civ. P. 23(a), (b)(1), (b)(2), (b)(3), and (c)(4).

64. **Numerosity:** The proposed Class is so numerous that joinder of all members is impracticable. Defendant has reported to the Indiana Attorney General's Office that the total number of individuals affected in the Data Breach was 318,558 individuals.[38]

65. **Typicality:** Plaintiff's claims are typical of the claims of the Class. Plaintiff and all members of the Class were injured through Empress EMS's uniform misconduct. The same event and conduct that gave rise to Plaintiff's claims are identical to those that give rise to the claims of every other Class member because Plaintiff and each member of the Class had their sensitive PII compromised in the same way by the same conduct of Empress EMS.

66. **Adequacy:** Plaintiff is an adequate representative of the Class because Plaintiff's interests do not conflict with the interests of the Class; Plaintiff has retained counsel competent and highly experienced in data breach class action litigation; and Plaintiff and Plaintiff's counsel intend to prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiff and his counsel.

67. **Superiority:** A class action is superior to other available means of fair and efficient adjudication of the claims of Plaintiff 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 members of the Class individually to effectively redress Empress EMS'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

[38] *See* "Data Breach Year-to-date Report April 2020," Indiana Attorney General, https://www.in.gov/attorneygeneral/files/Data%20Breach%20Year-to-date%20Report%20April%202020.pdf.

difficulties and provides benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

68. **Commonality and Predominance:** There are many questions of law and fact common to the claims of Plaintiff and the other members of the Class, and those questions predominate over any questions that may affect individual members of the Class. Common questions for the Class include:

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

b. Whether Defendant failed to adequately safeguard Plaintiff's and the Class's PII;

c. Whether Defendant owed a duty to Plaintiff and the Class to adequately protect their PII, and whether it breached this duty;

d. Whether Empress EMS breached its duties to Plaintiff and the Class as a result of the Data Breach;

e. Whether Empress EMS knew or should have known that its computer and network security systems were vulnerable to attacks;

f. Whether Empress EMS's conduct, including its failure to act, resulted in or was the proximate cause of the Breach;

g. Whether Empress EMS was negligent in permitting unencrypted PII off vast numbers of individuals to be stored within its inadequately protected network;

h. Whether Empress EMS was negligent in failing to adhere to reasonable retention policies, thereby greatly increasing the size of the Data Breach;

i. Whether Empress EMS breached implied contractual duties to Plaintiff and the Class to use reasonable care in protecting their PII;

j. Whether Empress EMS 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 Plaintiff and the Class;

k. Whether Empress EMS continues to breach duties to Plaintiff and the Class;

l. Whether Plaintiff and the Class suffered injury as a proximate result of Empress EMS's negligent actions or failures to act;

m. Whether Plaintiff and the Class are entitled to recover damages, equitable relief, and other relief; and

n. Whether Empress EMS's actions alleged herein constitute gross negligence, and whether Plaintiff and Class Members are entitled to punitive damages.

VI. CAUSES OF ACTION

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

69. Plaintiff incorporates by reference all preceding factual allegations as though fully alleged here.

70. Defendant Empress EMS solicited, gathered, and stored the PII of Plaintiff and the Class.

71. Defendant had full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and Class Members could and would suffer if the PII were wrongfully disclosed. Defendant had a duty to Plaintiff and each Class Member to exercise reasonable care in holding, safeguarding, and protecting that information. Plaintiff and the Class Members were the foreseeable victims of any inadequate safety and security practices. Plaintiff and the Class

Members had no ability to protect their PII that was in Empress EMS's possession. As such, a special relationship existed between Empress EMS and Plaintiff and the Class.

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

73. Defendant's duty extended to protecting Plaintiff 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 the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B. Numerous courts, including those in New York and the Second Circuit, and legislatures, including New York's, have recognized the existence of a specific duty owed by medical providers to reasonably safeguard the personal information of their patients.

74. Defendant had duties to protect and safeguard the PII of Plaintiff and the Class from being vulnerable to cyberattacks. Duties that Empress EMS owed Plaintiff and the Class include:

a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting the PII in its possession;
b. To protect the PII in its possession using reasonable and adequate security procedures and systems;
c. To adequately and properly audit, test, and train its employees to protect patient information;
d. To use adequate network security systems;

e. To adequately and properly audit, test, and train its employees regarding how to properly and securely transmit and store PII;

f. To implement processes to quickly detect a data breach, security incident, or intrusion; and

g. To promptly notify Plaintiff and Class Members of any data breach, security incident, or intrusion that affected or may have affected their PII.

75. Plaintiff and the Class were the intended beneficiaries of Defendant's duties, creating a special relationship between them and Empress EMS. Defendant was in a position to ensure that its systems were sufficient to protect the PII that Plaintiff and the Class had entrusted to it.

76. Defendant breached its duties of care by failing to adequately protect Plaintiff's and Class Members' PII. Defendant breached its duties by, among other things:

a. Failing to exercise reasonable care in obtaining, retaining securing, safeguarding, deleting, and protecting the PII in its possession;

b. Failing to protect the PII in its possession using reasonable and adequate security procedures and systems;

c. Failing to use adequate network security systems;

d. Failing to adequately and properly audit, test, and train its employees regarding how to properly and securely transmit and store PII;

e. Failing to consistently enforce security policies aimed at protecting Plaintiff and the Class's PII;

f. Failing to implement processes to quickly detect data breaches, security incidents, or intrusions;

g. Failing to abide by reasonable retention and destruction policies for PII; and

h. Failing to promptly and accurately notify Plaintiff and Class Members of the Data Breach that affected their PII, *see* N.Y. Gen. Bus. Law § 899-aa(2), (4).

77. Defendant's willful failure to abide by these duties was wrongful, reckless, and grossly negligent in light of the foreseeable risks and known threats.

78. As a proximate and foreseeable result of Defendant's grossly negligent conduct, Plaintiff and the Class have suffered damages and are at imminent risk of additional harms and damages (as alleged above).

79. The damages Plaintiff and the Class have suffered (as alleged above) were and are reasonably foreseeable.

80. The damages Plaintiff and the Class have and will suffer were and are the direct and proximate result of Defendant's grossly negligent conduct.

81. Plaintiff and the Class have suffered injury, including as described in Section IV.B, *supra*, and are entitled to actual and punitive damages in an amount to be proven at trial.

SECOND CAUSE OF ACTION
BREACH OF IMPLIED CONTRACT
(On Behalf of All Plaintiff and the Class)

82. Plaintiff incorporate by reference all preceding factual allegations as though fully alleged here.

83. Plaintiff and Class Members were required to provide Defendant with their PII, including their Social Security numbers.

84. When Plaintiff and Class Members provided their PII to Defendant when seeking medical services or employment, they entered into implied contracts in which Defendant agreed to comply with its statutory and common law duties to protect their PII and to timely notify them in the event of a Data Breach.

85. Based on Defendant's representations, legal obligations, and acceptance of Plaintiff's and the Class Members' PII, Defendant had an implied duty to safeguard their PII through the use of reasonable industry standards.

86. Defendant breached the implied contracts by failing to safeguard Plaintiff's and Class Members' PII and failing to provide them with timely and accurate notice of the Data Breach. Indeed, it took Empress EMS approximately three months to warn Plaintiff and Class Member of their imminent risk of identity theft. Defendant also failed to notify Plaintiff and the Class Members whether or not their driver's license numbers were compromised, leaving Plaintiff and Class Members unsure as to the extent of the information that was compromised.

87. As a direct and proximate result of Defendant's breach of implied contract, Plaintiff and the Class Members have suffered damages, including foreseeable consequential damages that Defendant knew about when it requested Plaintiff's and the Class Members' PII.

THIRD CAUSE OF ACTION
INJUNCTIVE AND DECLARATORY RELIEF
(On Behalf of all Plaintiff and the Class)

88. Plaintiff incorporates by reference all preceding factual allegations as though fully alleged here.

89. This count is brought under the Federal Declaratory Judgment Act, 28 U.S.C. § 2201.

90. As previously alleged and pleaded, Defendant owes duties of care to Plaintiff and Class Members that requires it to adequately secure their PII.

91. Defendant still possesses the PII of Plaintiff and the Class Members.

92. Defendant has not satisfied its contractual obligations and legal duties to Plaintiff and the Class Members.

93. Plaintiff, therefore, seeks 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 Defendant to engage third-party security auditors/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 Defendant to significantly increase its spending on cybersecurity including systems and personnel;
c. Ordering Defendant to engage third-party security auditors and internal personnel to run automated security monitoring;
d. Ordering that Defendant audit, test, and train their security personnel regarding any new or modified procedures;
e. Ordering that Defendant's segment Plaintiff's and the Class's PII 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;
f. Ordering that Defendant cease transmitting PII via unencrypted email;
g. Ordering that Defendant cease storing PII in email accounts;
h. Ordering that Defendant conduct regular database scanning and securing checks;
i. Ordering Defendant to 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;

j. Ordering Defendant to implement and enforce adequate retention policies for PII, including destroying, in a reasonably secure manner, PII once it is no longer necessary for the it to be retained; and

k. Ordering Defendant to meaningfully educate its current, former, and prospective employees and subcontractors about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps they must take to protect themselves.

VII. PRAYER FOR RELIEF

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

a. An order certifying this action as a class action under Fed. R. Civ. P. 23, defining the Class as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiff is are a proper representative of the Class requested herein;

b. A judgment in favor of Plaintiff and the Class awarding them appropriate monetary relief, including compensatory damages, punitive damages, attorney fees, expenses, costs, and such other and further relief as is just and proper;

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

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

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

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

VIII. DEMAND FOR JURY TRIAL

Plaintiff hereby demands a trial by jury on all appropriate issues raised in this Class Action Complaint.

Dated: October 14, 2022

Respectfully submitted,

/s/ *William B. Federman*
William B. Federman (S.D.N.Y. #WF9124)
FEDERMAN & SHERWOOD
10205 N. Pennsylvania Ave.
Oklahoma City, Oklahoma 73120
(405) 235-1560/ (405) 239-2112 (facsimile)
wbf@federmanlaw.com

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

Counsel for Plaintiff

**Pro Hac Vice* application to be submitted