Exhibit A1

UNITED STATES DISTRICT COURT
DISTRICT OF PUERTO RICO

JOSE A. MORALES ROSARIO, ZELMA ESTEVES ARRECHE, and DAPHNE I. CARRIÓN-LOZANO, individually and on behalf of all other similarly situated Plaintiffs, v. HOSPITAL ESPAÑOL AUXILIO MUTUO DE PUERTO RICO, INC., Defendant.	Case No: 3:25-cv-01244 **AMENDED CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

Plaintiffs, Jose A. Morales Rosario, Zelma Esteves Arreche, and Daphne I. Carrión-Lozano ("Plaintiffs") individually and on behalf of all others similarly situated ("Class Members"), bring this Amended Class Action Complaint against Defendant Hospital Español Auxilio Mutuo de Puerto Rico, Inc. dba Auxilio Mutuo Hospital ("Defendant" or "Auxilio Mutuo Hospital"), alleging as follows, based upon information and belief, investigation of counsel, and personal knowledge of Plaintiffs.

NATURE OF THE ACTION

1. This class action arises from Auxilio Mutuo Hospital's failure to protect highly sensitive data. The breach notification posted on Auxilio Mutuo Hospital's website is attached as Exhibit A (the "Breach Notice").[1] The breach notification Auxilio Mutuo Hospital sent Mr. Morales is attached as Exhibit B.

[1] Notificación Sobre Potencial Brecha de Datos, AUXILIO MUTUO, https://www.auxiliomutuo.com/notificacion-sobre-potencial-brecha-de-datos/ (last visited April 30, 2025).

2. Auxilio Mutuo Hospital did not discover on its own that its systems had been compromised, and despite outside expert help and the unreasonably amount of time that has passed, Auxilio Mutuo Hospital claims it is still unable to determine the scope of the Data Breach.

3. According to its Breach Notice, on September 23, 2023, the Department of Homeland Security informed the hospital that its systems were the likely target of a criminal cyber group (the "Data Breach"). Exs. A & B. After launching two investigations, the first concluding on November 21, 2023 and the second concluding on May 15, 2024, Auxilio Mutuo Hospital was able to limit the impacted patients to those who visited the hospital between August 2022 and September 2023. *Id.*

4. In its official Data Breach notice, Auxilio Mutuo Hospital disclosed that the Data Breach impacted individuals in, at least: Puerto Rico, the District of Columbia, Maryland, New Mexico, New York, North Carolina, Oregon, and Rhode Island.[2]

5. On or around April 21, 2025—***575 days after Homeland Security notified Auxilio Mutuo Hospital of the Data Breach***—Auxilio Mutuo Hospital finally began providing written notice of this incident. *Id.*

6. While the information impacted varies depending on the individual, the type of information potentially exposed includes personally identifying information, including names, dates of birth, Social Security numbers, driver's license numbers, state identification numbers, passport numbers, financial and banking information, account numbers, billing codes, payment

[2] *Notice of Potential Data Breach*, AUXILIO MUTUO, https://www.auxiliomutuo.com/en/notice-of-potential-data-breach/ (last visited July 22, 2025) (addressing the notice to "Maryland residents," "New Mexico residents," "New York residents," "North Carolina residents," "Oregon residents," and "Rhode Island residents").

cards, as well as protected health information including medical information and health insurance information. *Id.* Plaintiffs refer to the compromised data as "PII/PHI."

7. While Auxilio Mutuo Hospital does not state how long the Data Breach lasted, its Breach Notice suggests it was massive and lengthy. For an unknown period of time, cybercriminals accessed Auxilio Mutuo Hospital's system undetected, and were able to access patient data from possibly continuing from August 2022 to September 2023, evincing Auxilio Mutuo Hospital's grossly inadequate cybersecurity systems.

8. Moreover, the fact Auxilio Mutuo Hospital waited ***575 days*** from the date of the Homeland Security first notified it of the Data Breach, before it finally began notifying Class Members about the Data Breach, despite the fact that highly sensitive PII/PHI was compromised, evinces gross negligence.

9. Upon information and belief, cybercriminals were able to breach Auxilio Mutuo Hospital's systems because Auxilio Mutuo Hospital failed to adequately train its employees on cybersecurity, failed to adequately monitor its agents, contractors, vendors, and suppliers in handling and securing the PII/PHI of Plaintiffs, and failed to maintain reasonable security safeguards or protocols to protect the Class's PII/PHI—rendering it an easy target for cybercriminals.

10. The Breach Notice obfuscates the nature of the Data Breach and the threat it posed. Exs. A & B. The Breach Notice fails to disclose how many people were impacted, how the Data Breach happened, how long the Data Breach lasted, how cybercriminals were able to avoid detection for an unknown period of time, how the Department of Homeland Security was able to discover the Data Breach but Auxilio Mutuo Hospital was not, and why it took Auxilio Mutuo

Hospital more than 18 months before it finally began notifying some victims that cybercriminals had gained access to their highly private information.

11. Auxilio Mutuo Hospital's failure to timely report the Data Breach made the victims vulnerable to identity theft without any warnings to monitor their financial accounts or credit reports to prevent unauthorized use of their PII/PHI.

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

13. In failing to adequately protect the PII/PHI of individuals whose PII/PHI was in Auxilio Mutuo Hospital's custody and control, by failing to adequately notify them about the breach, and by obfuscating the nature of the breach, Auxilio Mutuo Hospital violated state law and harmed an unknown number of individuals.

14. Plaintiffs and the Class are victims of Auxilio Mutuo Hospital's negligence and inadequate cybersecurity measures. Specifically, Plaintiffs and members of the proposed Class trusted Auxilio Mutuo Hospital with their PII/PHI. But Auxilio Mutuo Hospital betrayed that trust when it failed to properly use industry-standard security practices to prevent the Data Breach.

15. Plaintiffs are victims of the Data Breach, having received a Breach Notice on or around April 21, 2025.

16. The exposure of one's PII/PHI to cybercriminals is a bell that cannot be unrung. Before the Data Breach, the private information of Plaintiffs and the Class was exactly that—private. Not anymore. Now, their private information is permanently exposed and unsecure.

17. Plaintiffs seek, on behalf of themselves and the Class, monetary damages and injunctive relief including lifetime credit monitoring and ID theft monitoring.

PARTIES

18. Plaintiff, Jose A. Morales Rosario, is a natural person and citizen of Puerto Rico, residing in Carolina, Puerto Rico, where he intends to remain. Mr. Morales Rosario is a Data Breach victim, receiving Notice of the Data Breach on or around April 21, 2025.

19. Plaintiff, Zelma Esteves Arreche, is a natural person and citizen of Puerto Rico, residing in Canovanas, Puerto Rico, where she intends to remain. She is a Data Breach victim, receiving Notice of the Data Breach on or around April 21, 2025.

20. Plaintiff, Daphne I. Carrión-Lozano, is a natural person and citizen of Puerto Rico, residing in Puerto Rico, where she intends to remain. She is a Data Breach victim, receiving Notice of the Data Breach on or around April 21, 2025.

21. Defendant Hospital Español Auxilio Mutuo de Puerto Rico, Inc. dba Auxilio Mutuo Hospital ("Defendant" or "Auxilio Mutuo Hospital"), is a domestic corporation headquartered at Ave Ponce de Leon 715, Parada 37.5, San Juan, Puerto Rico 00918.

JURISDICTION AND VENUE

22. This Court has subject matter jurisdiction over the claims asserted herein pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2), since some of the Class Members are citizens of a State different from the Defendants, there are more than 100 putative class members, and the amount in controversy exceeds $5 million. Minimal diversity exists because Defendant is a citizen of Puerto Rico, and Class Members are citizens of, *inter alia*, Puerto Rico, the District of Columbia, Maryland, New Mexico, New York, North Carolina, Oregon, and Rhode Island.[3]

[3] *Notice of Potential Data Breach*, AUXILIO MUTUO, https://www.auxiliomutuo.com/en/notice-of-potential-data-breach/ (last visited July 22, 2025) (addressing the notice to "Maryland residents," "New Mexico residents," "New York residents," "North Carolina residents," "Oregon residents," and "Rhode Island residents").

23. The Court has personal jurisdiction over Defendants because Plaintiffs' and Class Members' claims arise out of Defendants' business activities conducted in Puerto Rico, where Defendants' headquarters are located.

24. Venue is appropriate in this District because, among other things: (a) Plaintiffs resides in this District, (b) Defendant maintains offices in this District, where it conducts substantial business; (c) Defendant directed its activities at residents in this District; and (d) many of the acts and omissions that give rise to this Action took place in this judicial District.

25. Venue is further appropriate in this District pursuant to 28 U.S.C. § 1391 because Defendant conducts a large amount of their business in this District, and because Defendant has substantial relationships in this District.

BACKGROUND

Defendant Collected and Stored the PII/PHI of Plaintiffs and the Class

26. Auxilio Mutuo Hospital touts itself as the most comprehensive private hospital in Puerto Rico and the Caribbean, offering first class services and surgical procedures for more than 138 years.[4] Today, Auxilio Mutuo Hospital provides healthcare services in a range of medical areas, including cancer, cardiovascular, surgery, respiratory care, diabetes, dialysis, endoscopy, nuclear medicine, neurology, nutrition, pediatrics, rehabilitation, and more.[5] Located in San Juan, Puerto Rico, Auxilio Mutuo Hospital employs over 2,000 individuals.[6]

27. Given the nature of the services it provides, Auxilio Mutuo Hospital accumulates highly private PII/PHI of its current and former patients.

---

[4] About Us, AUXILIO GLOBAL HEALTH, https://www.auxilioglobal.com/about-us.php (last visited April 30, 2025).
[5] Servicios, AUXILIO MUTUO, https://www.auxiliomutuo.com (last visited April 30, 2025).
[6] *Id.*

28. In collecting and maintaining the PII/PHI of its current and former patients, Auxilio Mutuo Hospital agreed it would safeguard the data in accordance with state law and federal law. After all, Plaintiffs and Class Members themselves took reasonable steps to secure their PII/PHI.

29. Auxilio Mutuo Hospital understood the need to protect the PII/PHI of current and former patients, and the need to prioritize its data security. Indeed, Auxilio Mutuo Hospital represented in the Breach Notice posted on its Website that "We take privacy and security very seriously" (Ex. A) and contains a Privacy Policy purporting to safeguard patient data.[7]

30. On information and belief, Auxilio Mutuo Hospital has not implemented reasonable cybersecurity safeguards or policies to protect the PII/PHI of its employees, clients, and patients, or trained its IT or data security employees to prevent, detect, and stop breaches of its systems. As a result, Defendant leaves significant vulnerabilities in its systems for cybercriminals to exploit and gain access to the PII/PHI of its current and former patients.

Defendant Failed to Safeguard the PII/PHI of Plaintiffs and the Class

31. Upon information and belief, the Data Breach impacted residents of Puerto Rico, Maryland, New Mexico, New York, North Carolina, Oregon, and Rhode Island. Ex. A.

32. Plaintiffs received a Breach Notice on or around April 21, 2025, indicating their PII/PHI was potentially impacted by the massive and lengthy Data Breach.

33. On information and belief, Defendant collects and maintains the highly private PII/PHI of current and former patients, including information protected by HIPAA, unencrypted in its computer systems. Given the length of time it has been in business, it has accumulated approximately 138 years of patient and employee data.

---

[7] *Sign Up and Connect – Patient Portal,* AUXILIO MUTUO, *https://auxiliomutuo.followmyhealth.com/Login/Home/Index?authproviders=0&returnArea=PatientAccess#!/createNew* (last visited April 30, 2025).

34. In collecting and maintaining PII, Defendant implicitly agreed that it will safeguard the data using reasonable means according to state and federal law. It did not.

35. On or around July 13, 2024, Auxilio Mutuo Hospital issued a vague press release stating it discovered unauthorized access on its network on or around September 24, 2023.[8] It claimed "Although our investigation remains ongoing, we have concluded that a limited amount of personal information may have been removed from our network in connection with the incident, including full names and one or more of the following: medical records, diagnostic information, and other data related to patient care."[9] On information and belief, Auxilio Mutuo Hospital did not send written notification to potentially impacted individuals at this time, but instead encouraged "everyone to employe best security practices to protect personal information, including monitoring credit reports and financial statements."[10]

36. Auxilio Mutuo Hospital issued a second press release on April 21, 2025, explaining that the Department of Homeland Security notified it on September 23, 2023, that its systems could be the target of a cyberattack.[11] On November 21, 2023, Auxilio Mutuo Hospital's initial investigation revealed evidence consistent with unauthorized network access, although at that time, it claimed it could not determine if there had been any unauthorized data access or theft of information from its network.[12] *See also* Exs. A & B.

---

[8] Hospital Español Auxilio Mutuo de Puerto Rico, Inc. Reports Network Breach (July 13, 2024), EUROPEAN BUSINESS MAGAZINE, https://europeanbusinessmagazine.com/accessnewswire/hospital-espanol-auxilio-mutuo-de-puerto-rico-inc-reports-network-breach/ (last visited April 30, 2025).
[9] *Id.*
[10] *Id.*
[11] Notice of Data Breach (April 21, 2025), ACCESS NEWSWIRE, https://www.accessnewswire.com/newsroom/en/education/notice-of-data-breach-1017895 (last visited April 30, 2025).
[12] *Id.*

37. Auxilio Mutuo Hospital conducted a second investigation, and on May 15, 2024, where it identified evidence of unauthorized activity consistent with data exfiltration from systems that contained patient data, meaning it confirmed patient data was stolen.[13] On September 24, 2024, it claimed the breach was limited to patients who visited the hospital between August 2022 and September 2023.[14] *See also* Ex. A & B.

38. Despite the length of its two investigations, and despite its reliance on expert help, Auxilio Mutuo Hospital still remarkably maintains it is unable to determine the scope of the Data Breach, but admits that the stolen data potentially includes names in addition to some or all of the following:

- Contact information (first and last name, address, date of birth, phone number, and email address)
- Health information (medical record numbers, providers, diagnoses, medicines, test results, images, care and treatment information)
- Health insurance information (primary, secondary or other health plans/policies, insurance companies, member/group ID numbers, and Medicaid-Medicare-government payor ID numbers)
- Billing, claims, and payment information (claim numbers, account numbers, billing codes, payment cards, financial and banking information, payments made, and balance due)
- Other personal information (Social Security numbers, driver's licenses or state ID numbers, or passport numbers).[15] *See also* Exs. A & B.

[13] *Id.*
[14] *Id.*
[15] *Id.*

39. As evidenced by the Data Breach, Defendant's cybersecurity systems were completely inadequate and allowed cybercriminals to steal files containing a treasure trove of highly private information belonging to its patients.

40. To make matters worse, Defendant waited until April 21, 2025, or at least 575 days, before it started notifying victims of the Data Breach.

41. Thus, Defendant kept the Class in the dark for over a year—thereby depriving the Class of the opportunity to try and mitigate their injuries in a timely manner.

42. Despite its duties to safeguard PII/PHI, Defendant did not in fact follow industry standard practices in securing the PII/PHI of its current and former patients, as evidenced by the Data Breach, its failure to discover the Data Breach, its failure to determine the scope of the Data Breach, and its extreme delay in notifying victims.

43. In response to the Data Breach, Defendant vaguely contends that it has "taken steps to strengthen our network systems to reduce the risk of a similar incident occurring in the future." Exs. A & B. Although Defendant does not explain what "steps" it has taken, such measures, if implemented at all, should have been in place before the Data Breach.

44. Through its Notice, Defendant recognized the actual imminent harm and injury that flowed from the Data Breach, providing monitoring services, and advising Plaintiffs "to remain vigilant against incidents of identity theft and fraud by reviewing your credit reports and account statements for suspicious activity and to detect errors. Exs. A & B.

45. Despite recognizing the harm that flowed from the Data Breach, Defendant waited an unreasonable amount of time before it began notifying victims, depriving Plaintiffs and the Class of the earliest opportunity to take appropriate measures to protect their PII/PHI and take other necessary steps to mitigate the harm caused by the Data Breach.

46. On information and belief, Defendant has offered identity monitoring services to some victims, for twelve months, which does not adequately address the lifelong harm that victims will face following the Data Breach. Indeed, the information compromised involves PII/PHI that cannot be changed, such as Social Security numbers. Exs. A & B.

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

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

49. On information and belief, Defendant failed to adequately train its IT and data security employees on reasonable cybersecurity protocols or implement reasonable security measures, causing them to lose control over the PII/PHI of its employees, clients, and patients. Defendant's negligence is evidenced by its failure to prevent the Data Breach, failure to detect the Data Breach for an unknown period of time, and its inability to determine the exact information that was accessed, and the number of impacted individuals, for an unreasonable amount of time

50. Furthermore, Defendant obfuscates the nature of the Data Breach and the threat it posed. Exs. A & B. The Breach Notice fails to disclose how many people were impacted, how the Data Breach happened, how long the Data Breach lasted, how cybercriminals were able to avoid detection for an unknown period of time, how the Department of Homeland Security was able to

discover the Data Breach but Auxilio Mutuo Hospital was not, and why it took Auxilio Mutuo Hospital more than 18 months before it finally began notifying some victims that cybercriminals had gained access to their highly private information.

Defendant Knew—Or Should Have Known—of the Risk of a Data Breach

51. It is well known that PII/PHI is an invaluable commodity and a frequent target of hackers.

52. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in recent years.

53. In fact, out of twenty industries that were analyzed, the healthcare industry is number eleven for highest count of ransomware attacks from January 2022 to January 2023.[16]

54. In 2024, a 3,158 data breaches occurred, exposing approximately 1,350,835,988 sensitive records—a 211% increase year-over-year.[17]

55. Indeed, cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets, so they are aware of and take appropriate measures to prepare for and are able to thwart such an attack. 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."[18]

---

[16] *Ransomware Statistics: Who is targeted the most?* NORDLOCKER, https://nordlocker.com/ransomware-attack-statistics/ (last visited March 24, 2025).

[17] *2024 Data Breach Annual Report*, IDENTITY THEFT RESOURCE CENTER, https://www.idtheftcenter. org/publication/2024-data-breach-report/ (last visited March 24, 2025).

[18] Ben Kochman, *FBI, Secret Service Warn of Targeted Ransomware*, LAW360 (published Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware (last visited March 24, 2025).

56. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in the healthcare industry, including Defendant.

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

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

59. In light of the information readily available and accessible before the Data Breach, Defendant, knew or should have known that there was a foreseeable risk that Plaintiffs' and Class Members' PII/PHI could be accessed, exfiltrated, and published as the result of a cyberattack. Data breaches are so prevalent in today's society therefore making the risk of experiencing a data breach entirely foreseeable to Defendant.

Plaintiff Jose A. Morales Rosario's Experiences and Injuries

60. Plaintiff Jose A. Morales Rosario is a former patient of Auxilio Mutuo Hospital and is a Data Breach victim.

61. Plaintiff is very careful about sharing his PII/PHI, and he has never knowingly transmitted his PII/PHI over the internet (or via any other method) in an unsecure manner. Furthermore, Plaintiff is careful to store any documents containing his PII/PHI in a secure location.

62. According to the Breach Notice he received on or around April 21, 2025, his first and last name, in combination with the following data elements, may have been impacted in the Data Breach:

- Health information (medical record numbers, providers, diagnoses, medicines, test results, images, care and treatment information);
- Health insurance information (primary, secondary or other health plans/policies, insurance companies, member/group ID numbers, and Medicaid-Medicare-government payor ID numbers);
- Billing, claims, and payment information (claim numbers, account numbers, billing codes, payment cards, financial and banking information, payments made, and balance due); and
- Other personal information (Social Security numbers, driver's licenses or state ID numbers, or passport numbers).

63. As a condition of receiving services, Defendant required Plaintiff to provide his PII/PHI, including at least his name, date of birth, Social Security Number, and health information.

64. Plaintiff provided his PII/PHI to Defendant and trusted that the company would use reasonable measures to protect it according to state and federal law.

65. Additionally, Plaintiff reasonably expected that his personal information would be destroyed once his treatment from Defendant ended.

66. As a result of its inadequate cybersecurity measures and data destruction policies, Defendant exposed Plaintiff's PII/PHI for theft by cybercriminals and given the purpose of the hack, for sale on the Dark Web.

67. To make matters worse, Plaintiff's credit score inexplicably dropped by approximately eleven (11) points during 2025. Plaintiff is unsure what could have caused the drop in his credit score—apart from the misuse of his PII/PHI by cybercriminals (e.g., identity theft).

68. Thus, on information and belief, this drop was caused by the misuse of his PII/PHI (e.g., identity theft) by cybercriminals who obtained his PII/PHI from Defendant during the Data Breach.

69. Defendant deprived Plaintiff of the earliest opportunity to guard himself against the Data Breach's effects by failing to promptly notify him about the Data Breach.

70. Plaintiff suffered actual injury from the exposure of his PII/PHI —which violates his rights to privacy.

71. Plaintiff suffered actual injury in the form of damages to and diminution in the value of his PII/PHI. After all, PII/PHI is a form of intangible property—property that Defendant was required to adequately protect.

72. As a result of the Data Breach, Plaintiff has spent time and made reasonable efforts to mitigate its impact, including but not limited to researching the Data Breach, reviewing credit card and financial account statements and monitoring his credit information.

73. Plaintiff will continue to spend considerable time and effort monitoring his accounts to protect himself from identity theft. Plaintiff fears for his personal financial security and uncertainty over what PII/PHI was exposed. Plaintiff has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

74. Plaintiff is now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from his PII/PHI being placed in the hands of unauthorized third parties. This injury is worsened by Defendant's failure to promptly inform Plaintiff about the Data Breach.

75. Once an individual's PII/PHI is for sale and access on the Dark Web, cybercriminals are able to use the stolen and compromised to gather and steal even more information.[19] Plaintiff's PII/PHI was compromised as a result of the Data Breach.

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

77. Plaintiff also has a continuing interest in lifetime credit monitoring and identity theft monitoring on account of the Data Breach.

Plaintiff Zelma Esteves Arreche's Experiences and Injuries

78. Plaintiff is a patient of Auxilio Mutuo Hospital and is a Data Breach victim. She received several Data Breach notices—informing her that the Data Breach exposed the PII/PHI of herself and also her two (2) children.[20]

79. Plaintiff is very careful about sharing her PII/PHI (or the PII/PHI of her children), and she has never knowingly transmitted her PII/PHI (or the PII/PHI of her children) over the internet (or via any other method) in an unsecure manner. Furthermore, Plaintiff is careful to store any documents containing her PII/PHI (or the PII/PHI of her children) in a secure location.

---

[19] *What do Hackers do with Stolen Information,* AURA, https://www.aura.com/learn/what-do-hackers-do-with-stolen-information (last visited March 44, 2025).

[20] The Data Breach notice that Plaintiff received on behalf of one of her children is attached as Exhibit C. Portions of the child's name have been redacted to preserve their privacy.

80. According to the Breach Notices she received on or around April 21, 2025, her PII/PHI—and the PII/PHI of her children—were impacted in the Data Breach. The exposed PII/PHI included first and last names and the following:

- Health information (medical record numbers, providers, diagnoses, medicines, test results, images, care and treatment information);
- Health insurance information (primary, secondary or other health plans/policies, insurance companies, member/group ID numbers, and Medicaid-Medicare-government payor ID numbers);
- Billing, claims, and payment information (claim numbers, account numbers, billing codes, payment cards, financial and banking information, payments made, and balance due); and
- Other personal information (Social Security numbers, driver's licenses or state ID numbers, or passport numbers).

81. As a condition of receiving services, Defendant required Plaintiff to provide her PII/PHI—and the PII/PHI of her children—including at least names, dates of birth, Social Security numbers, and health information.

82. Plaintiff provided her PII/PHI (and the PII/PHI of her children) to Defendant and trusted that the company would use reasonable measures to protect it according to state and federal law.

83. Additionally, Plaintiff reasonably expected that her personal information would be destroyed once her treatment from Defendant ended.

84. As a result of its inadequate cybersecurity measures and data destruction policies, Defendant exposed the PII/PHI of Plaintiff and her children for theft by cybercriminals and given the purpose of the hack, for sale on the Dark Web.

85. Defendant deprived Plaintiff of the earliest opportunity to guard herself against the Data Breach's effects by failing to promptly notify her about the Data Breach.

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

87. Plaintiff suffered actual injury in the form of damages to and diminution in the value of her PII/PHI. After all, PII/PHI is a form of intangible property—property that Defendant was required to adequately protect.

88. As a result of the Data Breach, Plaintiff has spent time and made reasonable efforts to mitigate its impact, including but not limited to researching the Data Breach, reviewing credit card and financial account statements and monitoring her credit information.

89. Plaintiff will continue to spend considerable time and effort monitoring her accounts to protect himself from identity theft. Plaintiff fears for her personal financial security and uncertainty over what PII/PHI was exposed. Plaintiff has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

90. Plaintiff is now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from her PII/PHI being placed in the hands of unauthorized third parties. This injury is worsened by Defendant's failure to promptly inform Plaintiff about the Data Breach.

91. Once an individual's PII/PHI is for sale and access on the Dark Web, cybercriminals are able to use the stolen and compromised to gather and steal even more information.[21] Plaintiff's PII/PHI was compromised as a result of the Data Breach.

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

93. Plaintiff also has a continuing interest in lifetime credit monitoring and identity theft monitoring on account of the Data Breach.

94. Plaintiff suffered from the misuse of her PII/PHI when cybercriminals committed tax fraud for the 2023 and 2024 tax years using her Social Security number and the Social Security numbers of her two (2) children. More specifically:

a. Plaintiff was notified by the IRS that her Social Security number was already used to submit tax returns for the 2023 and 2024 tax years. In other words, cybercriminals used her Social Security number to commit identity theft.

b. Plaintiff was notified by the IRS that the Social Security numbers of her two children were used "on Form 1040-SS (PR) . . . as a Qualifying child SSN or Dependent SSN in a previously accepted tax return for the same tax period." As a result, Plaintiff was unable to claim her children as qualifying dependents on her tax returns (and thus, Plaintiff was unable to receive the associated child-related tax benefits).

[21] *What do Hackers do with Stolen Information,* AURA, https://www.aura.com/learn/what-do-hackers-do-with-stolen-information (last visited March 44, 2025).

95. On information and belief, these cybercriminals obtained the PII/PHI of Plaintiff and her children—including their Social Security numbers—from Defendant during the Data Breach. Then, these cybercriminals used the PII/PHI that they obtained from Defendant to steal the identities of Plaintiff and her children.

96. In an attempt to mitigate the fallout of such identity theft, Plaintiff filed an identity theft claim with the IRS for the 2024 tax year regarding the Social Security numbers that were fraudulently used by cybercriminals.

97. And on July 21, 2025, Plaintiff received a letter from the IRS confirming that:

a. "Your identity theft claim has been verified[.]"

b. "We placed an indicator on your 2024 tax account."

c. "We'll monitor your tax account for activity to help prevent future fraud."

d. "We'll review all tax returns with your Social Security number (SSN) for the possibility of identity theft."

e. "We placed an indicator on your account to alert us to make sure a tax return filed with your SSN is valid."

98. Plaintiff now spends approximately forty (40) hours per year attempting to mitigate the fallout of the misuse of her PII/PHI—including by contacting the IRS by phone and mail, gathering documents, researching how to mitigate identity theft, and monitoring her various accounts for signs of further identity theft or fraud.

Plaintiff Daphne I. Carrión-Lozano's Experiences and Injuries

99. Plaintiff is a patient of Auxilio Mutuo Hospital and is a Data Breach victim.

100. Plaintiff is very careful about sharing her PII/PHI, and she has never knowingly transmitted her PII/PHI over the internet (or via any other method) in an unsecure manner. Furthermore, Plaintiff is careful to store any documents containing her PII/PHI in a secure location.

101. According to the Breach Notice[22] she received on or around April 21, 2025, her first and last name, in combination with the following data elements, may have been impacted in the Data Breach:

- Health information (medical record numbers, providers, diagnoses, medicines, test results, images, care and treatment information);
- Health insurance information (primary, secondary or other health plans/policies, insurance companies, member/group ID numbers, and Medicaid-Medicare-government payor ID numbers);
- Billing, claims, and payment information (claim numbers, account numbers, billing codes, payment cards, financial and banking information, payments made, and balance due); and
- Other personal information (Social Security numbers, driver's licenses or state ID numbers, or passport numbers).

102. As a condition of receiving services, Defendant required Plaintiff to provide her PII/PHI, including at least her name, date of birth, Social Security Number, and health information.

103. Plaintiff provided her PII/PHI to Defendant and trusted that the company would use reasonable measures to protect it according to state and federal law.

104. Additionally, Plaintiff reasonably expected that her personal information would be destroyed once her treatment from Defendant ended.

[22] The data breach notice that she received is attached as Exhibit D.

105. As a result of its inadequate cybersecurity measures and data destruction policies, Defendant exposed Plaintiff's PII/PHI for theft by cybercriminals and given the purpose of the hack, for sale on the Dark Web.

106. Defendant deprived Plaintiff of the earliest opportunity to guard herself against the Data Breach's effects by failing to promptly notify him about the Data Breach.

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

108. Plaintiff suffered actual injury in the form of damages to and diminution in the value of her PII/PHI. After all, PII/PHI is a form of intangible property—property that Defendant was required to adequately protect.

109. As a result of the Data Breach, Plaintiff has spent time and made reasonable efforts to mitigate its impact, including but not limited to researching the Data Breach, reviewing credit card and financial account statements and monitoring her credit information.

110. Plaintiff will continue to spend considerable time and effort monitoring her accounts to protect himself from identity theft. Plaintiff fears for her personal financial security and uncertainty over what PII/PHI was exposed. Plaintiff has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

111. Plaintiff is now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from her PII/PHI being placed in the hands of unauthorized third parties. This injury is worsened by Defendant's failure to promptly inform Plaintiff about the Data Breach.

112. Once an individual's PII/PHI is for sale and access on the Dark Web, cybercriminals are able to use the stolen and compromised to gather and steal even more information.[23] Plaintiff's PII/PHI was compromised as a result of the Data Breach.

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

114. Plaintiff also has a continuing interest in lifetime credit monitoring and identity theft monitoring on account of the Data Breach.

115. To make matters worse, Plaintiff received a notification from her identity-monitoring service "MyIDCare" warning her that her PII/PHI was found "exposed on the dark web" on August 22, 2024. The warning further stated that:

a. "We monitor online activity to identify the potential illegal trading and selling of your personal information."

b. "Unfortunately, we found a match which indicates the information within the red box above is available online."

c. "The following data was found compromised with your Social Security number."

d. "Date Found: 08/22/2024."

116. In sum, MyIDCare warned Plaintiff that it found at least the following PII/PHI published on the Dark Web: first name, middle name, last name, address, city, state, zip code, and her Social Security number.

[23] *What do Hackers do with Stolen Information,* AURA, https://www.aura.com/learn/what-do-hackers-do-with-stolen-information (last visited March 44, 2025).

117. On information and belief, cybercriminals obtained Plaintiff's PII/PHI from Defendant during the Data Breach and then later published that PII/PHI on the Dark Web.

118. Thus, on information and belief, this drop was caused by the misuse of his PII/PHI (e.g., identity theft) by cybercriminals who obtained his PII/PHI because of the Data Breach.

119. Thereafter, Plaintiff was forced to spend time freezing her credit—to guard against further misuse of her identity and PII/PHI.

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

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

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

a. The loss of the opportunity to control how their PII/PHI is used;

b. The diminution in value of their PII/PHI;

c. The compromise and continuing publication of their PII/PHI;

d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

e. Lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen PII/PHI; and

h. The continued risk to their PII/PHI, which remains in the possession of Defendant and is subject to further breaches so long as Defendant fails to undertake the appropriate measures to protect the PII/PHI in its possession.

122. Stolen PII/PHI is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII/PHI can be worth up to $1,000.00 depending on the type of information obtained.

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

124. Social Security numbers are particularly attractive targets for hackers because they can easily be used to perpetrate identity theft and other highly profitable types of fraud. Moreover, Social Security numbers are difficult to replace, as victims are unable to obtain a new number until the damage is done.

125. It can take victims years to spot identity or PII/PHI theft, giving criminals plenty of time to use that information for cash.

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

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

128. The development of "Fullz" packages means that stolen PII/PHI from the Data Breach can easily be used to link and identify it to Plaintiffs' and the Class's phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII/PHI stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiffs and the Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiffs' and members of the Class's stolen PII/PHI is being misused, and that such misuse is fairly traceable to the Data Breach.

129. Defendant disclosed the PII/PHI of Plaintiffs and members of the proposed Class for criminals to use in the conduct of criminal activity. Specifically, Defendant opened up, disclosed, and exposed the PII/PHI of Plaintiffs and the Class to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, extortion, and exposure of stolen PII/PHI.

130. Defendant's failure to properly notify Plaintiffs and the Class of the Data Breach exacerbated Plaintiffs' and the Class's injuries by depriving them of the earliest opportunity to take appropriate measures to protect their PII/PHI and take other necessary steps to mitigate the harm caused by the Data Breach.

Consumers Prioritize Data Security

131. In 2024, the technology and communications conglomerate Cisco published the results of its multi-year "Consumer Privacy Survey."[24] Therein, Cisco reported the following:

a. "For the past six years, Cisco has been tracking consumer trends across the privacy landscape. During this period, privacy has evolved from relative obscurity to a customer requirement with more than 75% of consumer respondents saying they won't purchase from an organization they don't trust with their data."[25]

b. "Privacy has become a critical element and enabler of customer trust, with 94% of organizations saying their customers would not buy from them if they did not protect data properly."[26]

c. 89% of consumers stated that "I care about data privacy."[27]

d. 83% of consumers declared that "I am willing to spend time and money to protect data" and that "I expect to pay more" for privacy.[28]

e. 51% of consumers revealed that "I have switched companies or providers over their data policies or data-sharing practices."[29]

f. 75% of consumers stated that "I will not purchase from organizations I don't trust with my data."[30]

---

[24] *Privacy Awareness: Consumers Taking Charge to Protect Personal*, CISCO, https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-consumer-privacy-report-2024.pdf (last visited March 19, 2025).
[25] *Id*. at 3.
[26] *Id*.
[27] *Id*. at 9.
[28] *Id*.
[29] *Id*.
[30] *Id*. at 11.

Defendant Failed to Follow FTC Guidelines

132. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making. To that end, the FTC has issued numerous guidelines identifying best data security practices that businesses, such as Defendant, should employ to protect against the unlawful exposure of PII/PHI.

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

a. protect the personal customer information that they keep;

b. properly dispose of personal information that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

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

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

136. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an

unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

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

Defendant Failed to Follow Industry Standards

138. Several best practices have been identified that—at a minimum—should be implemented by businesses like Defendant. These industry standards include: educating all employees regarding cybersecurity; strong passwords; multi-layer security, including firewalls, anti-virus, and anti- malware software; encryption (making data unreadable without a key); multi-factor authentication; backup data; and limiting which employees can access sensitive data.

139. Other industry standard best practices include: installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

140. Upon information and belief, Defendant failed to implement industry-standard cybersecurity measures, including failing to meet the minimum standards of both the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical

Security Controls (CIS CSC), which are established standards in reasonable cybersecurity readiness.

141. These frameworks are applicable and accepted industry standards. And by failing to comply with these accepted standards, Defendant opened the door to the criminals—thereby causing the Data Breach.

Defendant Violated HIPAA

142. HIPAA provides specific privacy rules that require comprehensive administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of PII and PHI is properly maintained.[31]

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

a. failing to ensure the confidentiality and integrity of electronic PHI that it creates, receives, maintains and transmits in violation of 45 C.F.R. § 164.306(a)(1);

b. failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

c. failing to protect against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

d. failing to ensure compliance with HIPAA security standards by Defendant's workforce in violation of 45 C.F.R. § 164.306(a)(4);

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

e. failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

f. failing to implement policies and procedures to prevent, detect, contain and correct security violations in violation of 45 C.F.R. § 164.308(a)(1);

g. failing to identify and respond to suspected or known security incidents and failing to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. § 164.308(a)(6)(ii);

h. failing to effectively train all staff members on the policies and procedures with respect to PHI as necessary and appropriate for staff members to carry out their functions and to maintain security of PHI in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5); and

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

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

CLASS ACTION ALLEGATIONS

145. Plaintiffs bring this class action under Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3), individually and on behalf of all members of the following class:

> All individuals residing in the United States whose PII/PHI was compromised in the Data Breach of Auxilio Mutuo Hospital's network, including all those individuals who received notice of the breach.

146. Excluded from the Class are Defendant, its agents, affiliates, parents, subsidiaries, any entity in which Defendant has a controlling interest, any Defendant officer or director, any successor or assign, and any Judge who adjudicates this case, including its staff and immediate family.

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

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

149. This action satisfies the numerosity, commonality, typicality, and adequacy requirements.

150. **Numerosity.** The Class members are so numerous that joinder of all Class Members is impracticable. Upon information and belief, the proposed Class includes at least 8,496 members.

151. **Commonality and Predominance.** Plaintiffs' and the Class Members' claims raise predominantly common fact and legal questions—which predominate over any questions affecting individual Class Members—for which a class wide proceeding can answer for all Class Members. In fact, a class wide proceeding is necessary to answer the following questions:

a. if Defendant had a duty to use reasonable care in safeguarding Plaintiffs' and the Class's PII/PHI;

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

c. if Defendant was negligent in maintaining, protecting, and securing PII/PHI;

d. if Defendant breached contract promises to safeguard Plaintiffs and the Class's PII/PHI;

e. if Defendant took reasonable measures to determine the extent of the Data Breach after discovering it;

f. if Defendant's Breach Notice was reasonable;

g. if the Data Breach caused Plaintiffs and the Class injuries;

h. what the proper damages measure is; and

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

152. **Typicality.** Plaintiffs' claims are typical of Class Members' claims as each arises from the same Data Breach, the same alleged violations by Defendant, and the same unreasonable manner of notifying individuals about the Data Breach.

153. **Adequacy.** Plaintiffs will fairly and adequately protect the proposed Class's common interests. His interests do not conflict with Class Members' interests. And Plaintiffs has retained counsel—including lead counsel—that is experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf.

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

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

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

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

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

158. Defendant owed a duty of care to Plaintiffs and Class Members because it was foreseeable that Defendant's failure—to use adequate data security in accordance with industry standards for data security—would compromise their PII/PHI in a data breach. And here, that foreseeable danger came to pass.

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

160. Defendant owed these duties to Plaintiffs and Class Members because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security practices. After all, Defendant actively sought and obtained Plaintiffs' and Class Members' PII/PHI.

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

a. exercise reasonable care in handling and using the PII/PHI in its care and custody;

b. implement industry-standard security procedures sufficient to reasonably protect the information from a data breach, theft, and unauthorized;

c. promptly detect attempts at unauthorized access;

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

162. Also, Defendant owed a duty to timely and accurately disclose to Plaintiffs and Class Members the scope, nature, and occurrence of the Data Breach. After all, this duty is required and necessary for Plaintiffs and Class Members to take appropriate measures to protect their PII/PHI, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

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

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

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

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

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

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

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

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

a. disclosing and providing access to this information to third parties and

b. failing to properly supervise both the way the PII/PHI was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

171. Defendant breached its duties by failing to exercise reasonable care in supervising its agents, contractors, vendors, and suppliers, and in handling and securing the PII/PHI of Plaintiffs and Class Members which actually and proximately caused the Data Breach and Plaintiffs' and Class Members' injury.

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

173. Defendant has admitted that the PII/PHI of Plaintiffs and the Class was accessed by an intruder to its systems.

174. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiffs and Class Members have suffered or will suffer damages, including

monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

175. Defendant's breach of its common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiffs and Class Members actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their PII/PHI by criminals, improper disclosure of their PII/PHI, lost value of their PII/PHI, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendant's negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

SECOND CAUSE OF ACTION
Negligence *per se*
(On Behalf of Plaintiffs and the Class)

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

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

178. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect the PII/PHI entrusted to it. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiffs' and the Class Members' sensitive PII/PHI.

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

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

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

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

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

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

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

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

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

187. Defendant offered to provide services to Plaintiffs and members of the Class if, and in exchange, Plaintiffs and members of the Class provided Defendant with their PII/PHI.

188. In turn, Defendant agreed it would not disclose the PII/PHI it collects to unauthorized persons.

189. Plaintiffs and the members of the Class accepted Defendant's offer by providing PII/PHI to Defendant in exchange for Defendant's services.

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

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

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

a. Failing to properly safeguard and protect Plaintiffs' and members of the Class's PII/PHI;

b. Failing to comply with industry standards as well as legal obligations that are necessarily incorporated into the parties' agreement; and

c. Failing to ensure the confidentiality and integrity of electronic PII/PHI that Defendant created, received, maintained, and transmitted.

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

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

195. The covenant of good faith and fair dealing is an element of every contract. All such contracts impose upon each party a duty of good faith and fair dealing. The parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—not merely the letter—of the bargain. Put differently, the parties to a contract are mutually obligated to comply with the substance of their contract in addition to its form.

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

197. Defendant obfuscated the nature of the Data Breach and failed to send Notice to the victims promptly and sufficiently.

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

199. Plaintiffs and members of the Class have sustained damages because of Defendant's breaches of its agreement, including breaches of it through violations of the covenant of good faith and fair dealing.

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

FOURTH CAUSE OF ACTION
Unjust Enrichment
(On Behalf of Plaintiffs and the Class)

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

202. Plaintiffs restate and realleges all proceeding allegations above and hereafter as if fully set forth herein.

203. Upon information and belief, Defendant funds its data security measures from its general revenue, including payments made by or on behalf of Plaintiffs and the Class Members.

204. As such, a portion of the payments made by or on behalf of Plaintiffs and the Class Members is 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.

205. Plaintiffs and Class Members conferred a monetary benefit on Defendant. Specifically, they purchased services from Defendant and/or its agents and in so doing provided Defendant or its agents with their PII/PHI. In exchange, Plaintiffs and Class Members should have received from Defendant the goods and services that were the subject of the transaction and have their PII/PHI protected with adequate data security.

206. Defendant knew that Plaintiffs and Class Members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the PII/PHI of Plaintiffs and Class Members for business purposes.

207. Plaintiffs and Class Members conferred a monetary benefit on Defendant, by paying Defendant as part of Defendant rendering services, a portion of which was to have been used for data security measures to secure Plaintiffs' and Class Members' PII/PHI, and by providing Defendant with their valuable PII/PHI.

208. Defendant was enriched by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' PII/PHI. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant calculated to avoid the data security obligations at the expense of Plaintiffs and the Class by utilizing cheaper, ineffective security measures. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

209. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiffs and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

210. Defendant acquired the monetary benefit and PII/PHI through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

211. If Plaintiffs and Class Members knew that Defendant had not secured their PII/PHI, they would not have agreed to provide their PII/PHI to Defendant either directly or through their own financial institutions.

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

213. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) the loss of the opportunity how their PII/PHI is used; (ii) the compromise, publication, and/or theft of their PII/PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to 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 identity theft; (vi) the continued risk to their PII/PHI, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect PII/PHI in their 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 PII/PHI compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and the Class.

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

215. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, proceeds that it unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiffs and Class Members overpaid for Defendant's services.

FIFTH CAUSE OF ACTION
Invasion of Privacy
(On Behalf of Plaintiffs and the Class)

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

217. Plaintiffs and Class Members had a legitimate expectation of privacy regarding their PII/PHI and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

218. Specifically, Plaintiffs and Class Members had a reasonable expectation of privacy given Defendant's representations and Privacy Policy. Defendant's disclosure of Plaintiffs' PII is highly offensive to the reasonable person.

219. Defendant owed a duty to Plaintiffs and Class Member to keep their PII/PHI confidential.

220. The unauthorized disclosure and/or acquisition (i.e., theft) by a third party of Plaintiffs' and Class Members' PII/PHI, is highly offensive to a reasonable person. It constitute an invasion of privacy both by disclosure of nonpublic facts, and intrusion upon seclusion.

221. Defendant's reckless and negligent failure to protect Plaintiffs' and Class Members' PII/PHI constitutes an intentional interference with Plaintiffs' and the Class Members' interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

222. Defendant's failure to protect Plaintiffs' and Class Members' PII/PHI acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

223. Defendant knowingly did not notify Plaintiffs' and Class Members in a timely fashion about the Data Breach.

224. Because Defendant failed to properly safeguard Plaintiffs' and Class Members' PII/PHI, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiffs and the Class.

225. As a proximate result of Defendant's acts and omissions, the PII/PHI of Plaintiffs and the Class Members was stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiffs and the Class to suffer damages.

226. Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and the Class since their PII/PHI is still maintained by Defendant with their inadequate cybersecurity system and policies.

227. Plaintiffs and Class Members have no adequate remedy at law for the injuries relating to Defendant's continued possession of their PII/PHI. A judgment for monetary damages will not end Defendant's inability to safeguard the PII/PHI of Plaintiffs and the Class.

228. Plaintiffs and Class Members, seek injunctive relief to enjoin Defendant from further intruding into the privacy and confidentiality of Plaintiffs' and Class Members' PII/PHI.

229. Plaintiffs and Class Members seek compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, the costs of monitoring of their credit history for identity theft and fraud, plus prejudgment interest, and costs.

SIXTH CAUSE OF ACTION
Breach of Fiduciary Duty
(On Behalf of Plaintiffs and the Class)

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

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

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

233. Because of the highly sensitive nature of the PII/PHI, Plaintiffs and Class members (or their third-party agents) would not have entrusted Defendant, or anyone in Defendant's

position, to retain their PII/PHI had they known the reality of Defendant's inadequate data security practices.

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

235. Defendant also breached its fiduciary duties to Plaintiffs and Class members by failing to diligently discover, investigate, and give notice of the Data Breach within a reasonable and practicable time period.

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

SEVENTH CAUSE OF ACTION
Declaratory Judgment
(On Behalf of Plaintiffs and the Class)

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

190. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq*., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and to grant further necessary relief. The Court has broad authority to restrain acts, such as those alleged herein, which are tortious and unlawful.

191. In the fallout of the Data Breach, an actual controversy has arisen about Defendant's various duties to use reasonable data security. On information and belief, Plaintiffs alleges that Defendant's actions were—and *still* are—inadequate and unreasonable. And Plaintiffs and Class members continue to suffer injury from the ongoing threat of fraud and identity theft.

192. Given its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendant owed—and continues to owe—a legal duty to use reasonable data security to secure the data entrusted to it;

b. Defendant has a duty to notify impacted individuals of the Data Breach under the common law and Section 5 of the FTC Act;

c. That to comply with its obligations and duties of care, Defendant must implement and maintain reasonable security measures;

d. Defendant breached, and continues to breach, its duties by failing to use reasonable measures to the data entrusted to it; and

e. Defendant breaches of its duties caused—and continues to cause—injuries to Plaintiffs and Class members.

193. The Court should also issue corresponding injunctive relief requiring Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; (iii) immediately provide adequate life-time credit monitoring to all Class Members; and (iv) barring Defendant from disclosing the PII/PHI of Plaintiffs and the Class without their consent.

194. If an injunction is not issued, Plaintiffs and the Class Members will be protected from a second breach. Additionally, Plaintiffs and the Class will suffer irreparable injury, as their stolen information is more likely to be misused for identity theft or fraud without lifetime credit monitoring.

195. And if a second breach occurs, Plaintiffs and the Class will lack an adequate remedy at law because many of the resulting injuries are not readily quantified in full and they will be forced to bring multiple lawsuits to rectify the same conduct. Simply put, monetary damages—

while warranted for out-of-pocket damages and other legally quantifiable and provable damages—cannot cover the full extent of Plaintiffs and Class members' injuries.

196. If an injunction is not issued, the resulting hardship to Plaintiffs and Class members far exceeds the minimal hardship that Defendant could experience if an injunction is issued.

197. An injunction would benefit the public by preventing another data breach—thus preventing further injuries to Plaintiffs, Class members, and the public at large.

PRAYER FOR RELIEF

Plaintiffs and Class members respectfully request judgment against Defendant and that the Court enter an order:

A. Certifying this case as a class action on behalf of Plaintiffs and the proposed Class, appointing Plaintiffs as class representative, and appointing their counsel to represent the Class;

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

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

D. Enjoining Defendant from further unfair and/or deceptive practices;

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

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

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

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

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

J. Granting other relief that this Court finds appropriate.

DEMAND FOR JURY TRIAL

Plaintiffs demand a jury trial for all claims so triable.

Dated: September 10, 2025

By: */s/ Raina C. Borrelli*

Raina C. Borrelli (*Pro Hac Vice*)
Samuel J. Strauss (*Pro Hac Vice*)
STRAUSS BORRELLI PLLC
One Magnificent Mile
980 N. Michigan Ave., Suite 1610
Chicago, IL 60611
Telephone: (872) 263-1100
Facsimile: (872) 263-1109
raina@straussborrelli.com
sam@straussborrelli.com

Carlos E. Matos, Esq.
USDC-PR No.: 309902
Union Plaza Building, Suite 1202
416 Ponce de León Avenue
San Juan PR 00918
PO Box 11249
San Juan PR 00922-1249
(787) 378-1002
cemm787@gmail.com
LcdoMatos@pm.me

Attorneys for Plaintiffs and the Proposed Class

CERTIFICATE OF SERVICE

I, Raina C. Borrelli, hereby certify that on September 10, 2025, I electronically filed the foregoing with the Clerk of the Court using the CM/ECF system, which will send notification of such filing to counsel of record, via the ECF system.

DATED this 10th day of September, 2025.

STRAUSS BORRELLI PLLC

By: */s/ Raina C. Borrelli*

Raina C. Borrelli
STRAUSS BORRELLI PLLC
One Magnificent Mile
980 N. Michigan Ave., Suite 1610
Chicago, IL 60611
Telephone: (872) 263-1100
Facsimile: (872) 263-1109
raina@straussborrelli.com