UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS

NICOLE DELIA, on behalf of herself and all others similarly situated, Plaintiff, v. **HAH GROUP HOLDING COMPANY, LLC d/b/a HELP AT HOME**, Defendant.	Case No. 1:24-cv-07757 **CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

Nicole Delia ("Plaintiff"), through her attorneys, individually and on behalf of all others similarly situated, brings this Class Action Complaint against Defendant HAH Group Holding Company, LLC d/b/a Help At Home ("Help at Home" or "Defendant"), and its present, former, or future direct and indirect parent companies, subsidiaries, affiliates, agents, and/or other related entities. Plaintiff alleges the following on information and belief—except as to her own actions, counsel's investigations, and facts of public record.

NATURE OF ACTION

1. This class action arises from Defendant's failure to protect highly sensitive data.

2. Help at Home is a Chicago-based home care services company that serves tens of thousands of patients in 12 states.

3. As such, Defendant stores a litany of highly sensitive personal identifiable information ("PII") and private health information ("PHI") (collectively "Private Information") about its current and former patients. But Defendant lost control over that data when

cybercriminals infiltrated its insufficiently protected computer systems in a data breach (the "Data Breach").

4. Under state and federal law, organizations must report breaches involving PHI within at least sixty (60) days.

5. On or about August 16, 2024, Help at Home also sent out data breach letters to individuals whose information was compromised as a result of the hacking incident ("Breach Notice"). A sample of the Notice posted on Defendant's website is attached as Exhibit A.

6. Based on the Breach Notice sent to Plaintiff and "Class Members" (defined below), unusual activity was detected on its vendor's computer systems. In response, Defendant's vendor launched an investigation. Help at Home's investigation revealed that an unauthorized party had access to certain files that contained sensitive patient information, and that such access took place on or around March 21, 2024 (the "Data Breach"). Yet, Help at Home waited approximately five months to notify the public that they were at risk.

7. As a result of this delayed response, Plaintiff and Class Members had no idea for five months that their Private Information had been compromised, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm. The risk will remain for their respective lifetimes.

8. The Private Information compromised in the Data Breach contained highly sensitive patient data, representing a gold mine for data thieves. The data included, but is not limited to name, date of birth, Social Security number, financial account number, username and password, and/or certain medical, health insurance, and/or treatment information that Help at Home collected and maintained.

9. Armed with the Private Information accessed in the Data Breach (and a head start), data thieves can commit a variety of crimes including, *e.g.*, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' names to obtain medical services, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

10. There has been no assurance offered by Help at Home that all personal data or copies of data have been recovered or destroyed, or that Defendant has adequately enhanced its data security practices sufficient to avoid a similar breach of its network in the future.

11. Therefore, Plaintiff and Class Members have suffered and are at an imminent, immediate, and continuing increased risk of suffering, ascertainable losses in the form of harm from identity theft and other fraudulent misuse of their Private Information, the loss of the benefit of their bargain, out-of-pocket expenses incurred to remedy or mitigate the effects of the Data Breach, and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach.

12. Plaintiff brings this class action lawsuit to address Help at Home's inadequate safeguarding of Class Members' Private Information that it collected and maintained, and its failure to provide timely and adequate notice to Plaintiff and Class Members of the types of information that were accessed, and that such information was subject to unauthorized access by cybercriminals.

13. The potential for improper disclosure and theft of Plaintiff's and Class Members' Private Information was a known risk to Help at Home, and thus Help at Home was on notice that failing to take necessary steps to secure the Private Information left it vulnerable to an attack.

14. Upon information and belief, Help at Home failed to properly monitor and implement security practices with regard to the computer network and systems that housed the Private Information. Had Help at Home properly monitored the networks that store its patients' Private Information, it would have discovered the Breach sooner.

15. Plaintiff's and Class Members' identities are now at risk because of Help at Home's negligent conduct as the Private Information that Help at Home collected and maintained is now in the hands of data thieves and other unauthorized third parties.

16. Plaintiff seeks to remedy these harms on behalf of herself and all similarly situated individuals whose Private Information was accessed and/or compromised during the Data Breach.

17. Accordingly, Plaintiff, on behalf of herself and the Class, asserts claims for negligence, breach of contract, breach of implied contract, unjust enrichment, breach of fiduciary duty, breach of confidence, and declaratory judgment.

PARTIES

18. Plaintiff Nicole Delia is, and at all times mentioned herein was, an individual citizen of the State of New York.

19. Defendant HAH Group Holding, LLC is a home care service company incorporated in Delaware with its principal place of business at 33 S. State Street, Chicago, Illinois, 60603.

JURISDICTION AND VENUE

20. The Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of

interest and costs. Upon information and belief, the number of class members is over 100, many of whom have different citizenship from Help at Home. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

21. This Court has jurisdiction over Help at Home because Help at Home operates in and/or is incorporated in this District.

22. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events giving rise to this action occurred in this District and Help at Home has harmed Class Members residing in this District.

BACKGROUND

Defendant Collected and Stored the Private Information of Plaintiff and the Class

23. Help at Home is a home care services company. Founded in 1975, Help at Home is a leading U.S. home care provider that specializes in home care and home health services serving thousands of patients in at least 12 states.[1] Upon information and belief, Help at Home employs more than 49,000 people and generates approximately $3 billion in annual revenue.[2]

24. As a condition of receiving home care services, Help at Home requires that its patients entrust it with highly sensitive personal and health information. In the ordinary course of receiving service from Help at Home, Plaintiff and Class Members were required to provide their Private Information to Defendant.

25. In its notice letter, Help at Home states that it "values and respects the privacy of your information." Ex. A.

[1] https://www.helpathome.com/about/ (last visited August 27, 2024).
[2] https://www.zoominfo.com/c/help-at-home-llc/348727434 (last visited August 27, 2024).

26. In its Privacy Policy, Help at Home promises its patients that it is "committed to managing all data, including personally identifiable information, in accordance with all relevant laws and regulations[.]"[3]

27. Thus, due to the highly sensitive and personal nature of the information Help at Home acquires and stores with respect to its patients, Help at Home, upon information and belief, promises to, among other things: keep patients' Private Information private; comply with industry standards related to data security and the maintenance of its patients' Private Information; inform its patients of its legal duties relating to data security and comply with all federal and state laws protecting patients' Private Information; only use and release patients' Private Information for reasons that relate to the services it provides; and provide adequate notice to patients if their Private Information is disclosed without authorization.

28. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, Help at Home assumed legal and equitable duties it owed to them and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' Private Information from unauthorized disclosure and exfiltration.

29. Plaintiff and Class Members relied on Help at Home to keep their Private Information confidential and securely maintained and to only make authorized disclosures of this Information, which Defendant ultimately failed to do.

Defendant's Data Breach

[3] *See* https://www.helpathome.com/privacy-policy/ (last visited Aug. 21, 2024).

30. According to Defendant's Notice, it learned of unauthorized access to its vendor's computer systems on March 21, 2024, with such unauthorized access having taken place between on or around the same date.

31. Through the Data Breach, the unauthorized cybercriminal(s) accessed a cache of highly sensitive Private Information, including name, date of birth, Social Security number, financial account number, username and password, and/or certain medical, health insurance, and/or treatment information.

32. On or about August 16, 2024, roughly five months after Help at Home learned that the Class's Private Information was first accessed by cybercriminals, Help at Home finally began to notify patients that its vendor's investigation determined that their Private Information was included.

33. Help at Home had obligations created by contract, industry standards, common law, and representations made to Plaintiff and Class Members to keep Plaintiff's and Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

34. Plaintiff and Class Members provided their Private Information to Help at Home with the reasonable expectation and mutual understanding that Help at Home would comply with its obligations to keep such Information confidential and secure from unauthorized access and to provide timely notice of any security breaches.

35. Help at Home's data security obligations were particularly important given the substantial increase in cyberattacks in recent years.

36. Help at Home knew or should have known that its vendor's electronic records would be targeted by cybercriminals.

Plaintiff's Experiences and Injuries

37. Plaintiff Nicole Delia is a current patient of the Help at Home.

38. Thus, Defendant obtained and maintained Plaintiff's Private Information. And as a result, Plaintiff was injured by Defendant's Data Breach.

39. Plaintiff provided her Private Information to Defendant and trusted the company would use reasonable measures to protect it according to Defendant's internal policies, as well as state and federal law. Defendant obtained and continues to maintain Plaintiff's Private Information and has a continuing legal duty and obligation to protect that Private Information from unauthorized access and disclosure.

40. Plaintiff reasonably understood that a portion of the funds paid to Defendant in exchange for health services would be used to pay for adequate cybersecurity and protection of Private Information.

41. Upon information and belief, through its Data Breach, Defendant compromised Plaintiff's Private Information, including but not limited to her Social Security number, medical information, and date of birth. And upon information and belief, Plaintiff's Private Information has already been published—or will be published imminently—by cybercriminals on the Dark Web.

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

43. Because of Defendant's Data Breach, Plaintiff has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, Plaintiff's injuries are precisely the type of injuries that the law contemplates and addresses.

44. Plaintiff suffered actual injury from the exposure and theft of her Private Information—which violates her rights to privacy.

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

46. Plaintiff suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because Defendant's Data Breach placed Plaintiff's Private Information right in the hands of criminals.

47. Indeed, following the Data Breach, Plaintiff has suffered from a dramatic increase in daily spam phone calls and phishing emails inquiring about her Social Security number.

48. Further, following the Data Breach, Plaintiff experienced multiple instances of fraud in the form of fraudulent charges on her credit card between March and May 2024. As a result, Plaintiff was forced to close her credit card account.

49. Since the Data Breach, Plaintiff has also suffered an immense drop in her credit score, with her score rapidly plummeting into the 300 range.

50. Because of the Data Breach, Plaintiff anticipates spending considerable amounts of time and money to try and mitigate her injuries.

51. Today, Plaintiff has a continuing interest in ensuring that her Private Information—which, upon information and belief, remains backed up in Defendant's possession—is protected and safeguarded from additional breaches.

The Healthcare Sector is Particularly Susceptible to Data Breaches

52. Help at Home was on notice that companies in the healthcare industry are susceptible targets for data breaches.

53. Help at Home was also on notice that the FBI has 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 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 (PHI)."[4]

54. The American Medical Association ("AMA") has also warned healthcare companies about the importance of protecting their patients' confidential information: Cybersecurity is not just a technical issue; it's a patient safety issue. AMA research has revealed that 83% of physicians work in a practice that has experienced some kind of cyberattack. Unfortunately, practices are learning that cyberattacks not only threaten the privacy and security of patients' health and financial information, but also patient access to care.[5]

55. The healthcare sector reported the second largest number of data breaches among all measured sectors in 2018, with the highest rate of exposure per breach.[6] In 2022, the largest growth in compromises occurred in the healthcare sector.[7]

---

[4] Jim Finkle, FBI Warns Healthcare Firms that they are Targeted by Hackers, Reuters (Aug. 2014), available at https://www.reuters.com/article/us-cybersecurity-healthcare-fbi/fbi-warns-healthcare-firms-they-are-targeted-by- hackers-idUSKBN0GK24U20140820 (last visited on Aug. 21, 2024).

[5] Andis Robeznieks, Cybersecurity: Ransomware attacks shut down clinics, hospitals, Am. Med. Ass'n. (Oct. 4, 2019), available at: https://www.ama-assn.org/practice-management/sustainability/cybersecurity-ransomware- attacks-shut-down-clinics-hospitals (last visited on Aug. 21, 2024).

[6] Identity Theft Resource Center, 2018 End-of-Year Data Breach Report, available at: https://www.idtheftcenter.org/2018-data-breaches/ (last visited on Aug. 21, 2024).

[7] Identity Theft Resource Center, 2022 End-of-Yeare Data Breach Report, available at: https://www.idtheftcenter.org/wp-content/uploads/2023/01/ITRC_2022-Data-Breach-Report_Final-1.pdf (last visited on Aug. 21, 2024).

56. Indeed, when compromised, healthcare related data is among the most sensitive and personally consequential. A report focusing on healthcare breaches found that the "average total cost to resolve an identity theft-related incident … came to about $20,000," and that the victims were often forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[8]

57. Almost 50 percent of the victims lost their healthcare coverage as a result of the incident, while nearly 30 percent said their insurance premiums went up after the event. Forty percent of the customers were never able to resolve their identity theft at all. Data breaches and identity theft have a crippling effect on individuals and detrimentally impact the economy as a whole.[9]

58. Healthcare related breaches have continued to rapidly increase because electronic patient data is seen as a valuable asset. "Hospitals have emerged as a primary target because they sit on a gold mine of sensitive personally identifiable information for thousands of patients at any given time. From social security and insurance policies, to next of kin and credit cards, no other organization, including credit bureaus, have so much monetizable information stored in their data centers."[10]

59. As a healthcare provider, Help at Home knew, or should have known, the importance of safeguarding its patients' Private Information, including PHI, entrusted to it, and of the foreseeable consequences if such data were to be disclosed. These consequences include the

---

[8] Elinor Mills, Study: Medical identity theft is costly for victims, CNET (March 3, 2010), available at: https://www.cnet.com/news/privacy/study-medical-identity-theft-is-costly-for-victims/ (last visited on Aug. 21, 2024).

[9] *Id.*

[10] Inside Digital Health, How to Safeguard Hospital Data from Email Spoofing Attacks, April 4, 2019, available at: https://www.chiefhealthcareexecutive.com/view/how-to-safeguard-hospital-data-from-email-spoofing-attacks (last visited on Aug. 21, 2024).

significant costs that would be imposed on Help at Home's patients as a result of a breach. Help at Home failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring.

Help at Home Failed to Comply with HIPAA

60. Title II of HIPAA contains what are known as the Administration Simplification provisions. See 42 U.S.C. §§ 1301, et seq. These provisions require that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling PHI similar to the data Defendant left unguarded and vulnerable to attack. The HHS has subsequently promulgated five rules under authority of the Administrative Simplification provisions of HIPAA.

61. Help at Home's Data Breach resulted from a combination of insufficiencies that indicate Help at Home failed to comply with safeguards mandated by HIPAA regulations and industry standards. First, it can be inferred from Help at Home's Data Breach that Help at Home either failed to implement, or inadequately implemented, information security policies or procedures to protect Plaintiff's and Class Members' PHI.

62. Plaintiff's and Class Members' Private Information compromised in the Data Breach included "protected health information" as defined by CFR § 160.103.

63. 45 CFR § 164.402 defines "breach" as "the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information."

64. 45 CFR § 164.402 defines "unsecured protected health information" as "protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the [HHS] Secretary[.]"

65. Plaintiff's and Class Members' Private Information included "unsecured protected health information" as defined by 45 CFR § 164.402.

66. Plaintiff's and Class Members' unsecured PHI was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E, as a result of the Data Breach.

67. Based upon Defendant's Notice to Plaintiff and Class Members, Help at Home reasonably believes that Plaintiff's and Class Members' unsecured PHI has been acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E, as a result of the Data Breach.

68. Plaintiff's and Class Members' unsecured PHI that was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach was not rendered unusable, unreadable, or indecipherable to unauthorized persons.

69. Help at Home reasonably believes that Plaintiff's and Class Members' unsecured PHI that was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach was not rendered unusable, unreadable, or indecipherable to unauthorized persons.

70. Plaintiff's and Class Members' unsecured PHI that was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach, and which was not rendered unusable, unreadable, or indecipherable to unauthorized persons, was viewed by unauthorized persons.

71. Plaintiff's and Class Members' unsecured PHI was viewed by unauthorized persons in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach.

72. Help at Home reasonably believes that Plaintiff's and Class Members' unsecured PHI was viewed by unauthorized persons in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach.

73. It is reasonable to infer that Plaintiff's and Class Members' unsecured PHI that was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach, and which was not rendered unusable, unreadable, or indecipherable to unauthorized persons, was viewed by unauthorized persons.

74. It should be rebuttably presumed that unsecured PHI acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E, and which was not rendered unusable, unreadable, or indecipherable to unauthorized persons, was viewed by unauthorized persons.

75. After receiving notice that they were victims of the Data Breach (which required the filing of a data breach report in accordance with 45 CFR § 164.408(a)), it is reasonable for recipients of that notice, including Plaintiff and Class Members in this case, to believe that future harm (including medical identity theft) is real and imminent, and to take steps necessary to mitigate that risk of future harm.

76. In addition, Help at Home's Data Breach could have been prevented if Help at Home had implemented HIPAA mandated, industry standard policies and procedures for securely disposing of PHI when it was no longer necessary and/or had honored its obligations to its patients.

77. Help at Home's security failures also include, but are not limited to:

a. Failing to maintain an adequate data security system to prevent data loss;

b. Failing to mitigate the risks of a data breach and loss of data;

c. Failing to ensure the confidentiality and integrity of electronic protected health information Help at Home creates, receives, maintains, and transmits in violation of 45 CFR 164.306(a)(1);

d. Failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights in violation of 45 CFR 164.312(a)(1);

e. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 CFR 164.308(a)(1);

f. Failing to identify and respond to suspected or known security incidents;

g. Failing to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity, in violation of 45 CFR 164.308(a)(6)(ii);

h. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic protected health information, in violation of 45 CFR 164.306(a)(2);

i. Failing to protect against any reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 CFR 164.306(a)(3);

j. Failing to ensure compliance with HIPAA security standard rules by Defendant's workforce, in violation of 45 CFR 164.306(a)(94); and

k. Impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons, in violation of 45 CFR 164.502, et seq.

78. The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414 also required Help at Home to provide notice of the Data Breach to each affected individual "without unreasonable delay and in no case later than 60 days following discovery of the breach" (emphasis added).

79. Because Help at Home has failed to comply with HIPAA, while monetary relief may cure some of Plaintiff's and Class Members' injuries, injunctive relief is also necessary to ensure Help at Home's approach to information security is adequate and appropriate going forward. Help at Home still maintains the PHI and other highly sensitive Private Information of its current and former patients, including Plaintiff and Class Members. Without the supervision of the Court through injunctive relief, Plaintiff's and Class Members' Private Information remains at risk of subsequent data breaches.

Help at Home Failed to Comply with FTC Guidelines

80. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision making. Indeed, the FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. See, e.g., FTC v. Wyndham Worldwide Corp., 799 F.3d 236 (3d Cir. 2015).

81. In October 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cybersecurity guidelines for businesses. The guidelines

note that businesses should protect the personal customer 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 to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs, monitor all incoming traffic for activity indicating someone is attempting to hack into the system, watch for large amounts of data being transmitted from the system, and have a response plan ready in the event of a breach.

82. The FTC further recommends that companies not maintain Private 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 the network for suspicious activity, and verify that third-party service providers have implemented reasonable security measures.

83. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data by 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 the FTCA. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

84. As evidenced by the Data Breach, Help at Home failed to properly implement basic data security practices. Help at Home's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiff's and Class Members' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

85. Help at Home was at all times fully aware of its obligation to protect the Private Information of its patients yet failed to comply with such obligations. Defendant was also aware of the significant repercussions that would result from its failure to do so.

Help at Home Failed to Comply with Industry Standards

86. As noted above, experts studying cybersecurity routinely identify businesses as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

87. Some industry best practices that should be implemented by businesses dealing with sensitive PHI like Help at Home include but are not limited to: educating all employees, strong password requirements, multilayer security including firewalls, anti-virus and anti-malware software, encryption, multi-factor authentication, backing up data, and limiting which employees can access sensitive data. As evidenced by the Data Breach, Defendant failed to follow some or all of these industry best practices.

88. Other best cybersecurity practices that are standard in the industry include: installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protecting physical security systems; and training staff regarding these points. As evidenced by the Data Breach, Defendant failed to follow these cybersecurity best practices.

89. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for

Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

90. Defendant failed to comply with these accepted standards, thereby permitting the Data Breach to occur.

Help at Home Breached its Duty to Safeguard Plaintiff's and Class Members' Private Information

91. In addition to its obligations under federal and state laws, Help at Home owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Help at Home owed a duty to Plaintiff and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected the Private Information of Class Members.

92. Help at Home breached its obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard the computer systems that housed Plaintiff's and Class Members' data. Help at Home's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system that would reduce the risk of data breaches and cyberattacks;

b. Failing to adequately protect patients' Private Information;

c. Failing to properly monitor its vendor's data security systems for existing intrusions;

d. Failing to fully comply with FTC guidelines for cybersecurity in violation of the FTCA;

e. Failing to adhere to HIPAA and industry standards for cybersecurity as discussed above; and

f. Otherwise breaching its duties and obligations to protect Plaintiff's and Class Members' Private Information.

93. Help at Home negligently and unlawfully failed to safeguard Plaintiff's and Class Members' Private Information by allowing cyberthieves to access the computer network and systems which contained unsecured and unencrypted Private Information.

94. Had Help at Home remedied the deficiencies in the information storage and security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, it could have prevented intrusion into its information storage and security systems and, ultimately, the theft of Plaintiff's and Class Members' confidential Private Information.

95. Accordingly, Plaintiff's and Class Members' lives were severely disrupted. What's more, they have been harmed as a result of the Data Breach and now face an increased risk of future harm that includes, but is not limited to, fraud and identity theft. Plaintiff and Class Members also lost the benefit of the bargain they made with Help at Home.

Help at Home Should Have Known that Cybercriminals Target PII and PHI to Carry Out Fraud and Identity Theft

96. The FTC hosted a workshop to discuss "informational injuries," which are injuries that consumers like Plaintiff and Class Members suffer from privacy and security incidents such as data breaches or unauthorized disclosure of data.[11] Exposure of highly sensitive personal

[11] FTC Information Injury Workshop, BE and BCP Staff Perspective, Federal Trade Commission, (October 2018), available at https://www.ftc.gov/system/files/documents/reports/ftc-informational-injury-workshop-be-bcp-staff-perspective/informational_injury_workshop_staff_report_-_oct_2018_0.pdf (last visited on Aug. 21, 2024).

information that a consumer wishes to keep private may cause harm to the consumer, such as the ability to obtain or keep employment. Consumers' loss of trust in e-commerce also deprives them of the benefits provided by the full range of goods and services available which can have negative impacts on daily life.

97. Any victim of a data breach is exposed to serious ramifications regardless of the nature of the data that was breached. Indeed, the reason why criminals steal information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims or to take over victims' identities in order to engage in illegal financial transactions under the victims' names.

98. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity or to otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

99. In fact, as technology advances, computer programs may scan the Internet with a wider scope to create a mosaic of information that may be used to link compromised information to an individual in ways that were not previously possible. This is known as the "mosaic effect." Names and dates of birth, combined with contact information like telephone numbers and email addresses, are very valuable to hackers and identity thieves as it allows them to access users' other accounts.

100. Thus, even if certain information was not purportedly involved in the Data Breach, the unauthorized parties could use Plaintiff's and Class Members' Private Information to access accounts, including, but not limited to, email accounts and financial accounts, to engage in a wide variety of fraudulent activity against Plaintiff and Class Members.

101. One such example of this is the development of "Fullz" packages.

102. Cybercriminals can cross-reference two sources of the Private Information compromised in the Data Breach 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.

103. The development of "Fullz" packages means that the stolen Private Information from the Data Breach can easily be used to link and identify it to Plaintiff's and the proposed Class's phone numbers, email addresses, and other sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card or financial account numbers may not be included in the Private Information stolen 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 Plaintiff and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff and other Class Members' stolen Private Information is being misused, and that such misuse is fairly traceable to the Data Breach.

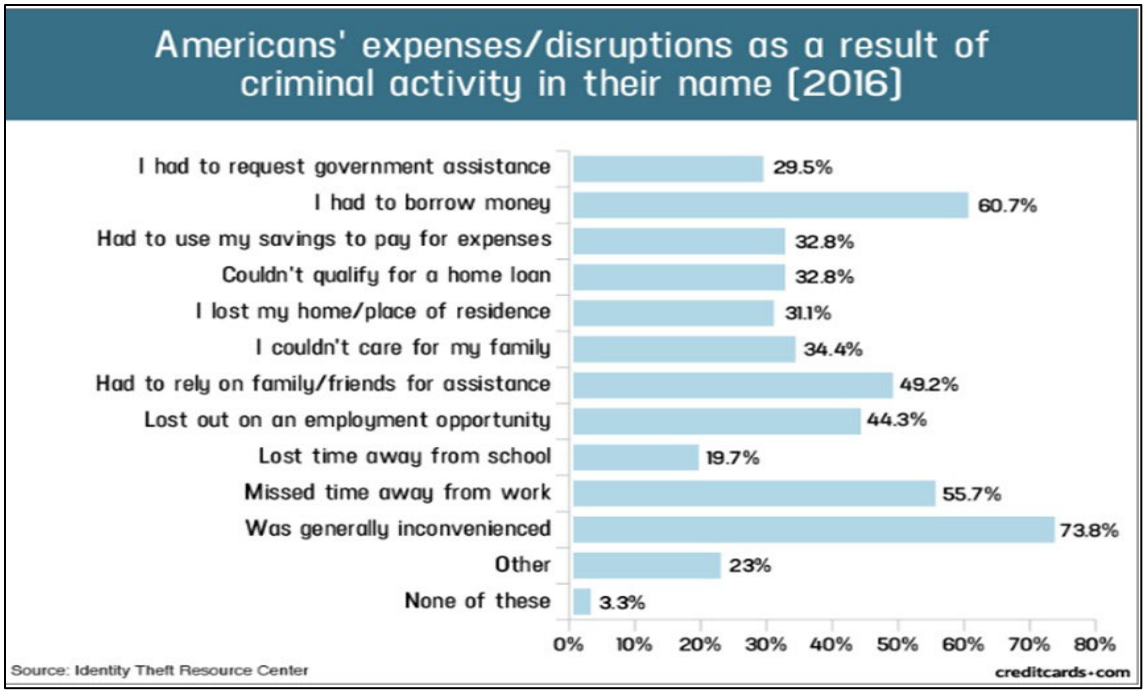
104. For these reasons, the FTC recommends that identity theft victims take several time-consuming steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert on their account (and an extended fraud alert that lasts for 7 years if someone steals the victim's identity), reviewing their

credit reports, contacting companies to remove fraudulent charges from their accounts, placing a freeze on their credit, and correcting their credit reports.[12] However, these steps do not guarantee protection from identity theft but can only mitigate identity theft's long-lasting negative impacts.

105. Identity thieves can also use stolen personal information such as Social Security numbers and PHI for a variety of crimes, including credit card fraud, phone or utilities fraud, bank fraud, to obtain a driver's license or official identification card in the victim's name but with the thief's picture, to obtain government benefits, or to file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house in the victim's name, receive medical services in the victim's name, and even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

106. In fact, a study by the Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of PII[13]:

[12] See IdentityTheft.gov, Federal Trade Commission, available at https://www.identitytheft.gov/Steps (last visited Aug. 21, 2024).
[13] Steele, Jason, Credit Card and ID Theft Statistics, CreditCards.com (October 23, 2017), available at https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276/ (last visited on Aug. 21, 2024).



107. PHI is also especially valuable to identity thieves. As the FTC recognizes, identity thieves can use PHI to commit an array of crimes, including identity theft and medical and financial fraud.[14]

108. Indeed, a robust cyber black market exists in which criminals openly post stolen PHI on multiple underground Internet websites, commonly referred to as the dark web.

109. While credit card information and associated PII can sell for as little as $1-$2 on the black market, protected health information can sell for as much as $363 according to the Infosec Institute.[15]

110. PHI is particularly valuable because criminals can use it to target victims with frauds and scams that take advantage of the victim's medical conditions or victim settlements. It

[14] Federal Trade Commission, *Warning Signs of Identity Theft, available at*: https://consumer.ftc.gov/articles/what- know-about-identity-theft (last visited on Aug. 21, 2024).
[15] Center for Internet Security, *Data Breaches: In the Healthcare Sector, available at*: https://www.cisecurity.org/insights/blog/data-breaches-in-the-healthcare-sector (last visited on Aug. 21, 2024).

can be used to create fake insurance claims, allowing for the purchase and resale of medical equipment, or gain access to prescriptions for illegal use or resale.

111. Medical identity theft can result in inaccuracies in medical records and costly false claims. It can also have life-threatening consequences. If a victim's health information is mixed with other records, it can lead to misdiagnosis or mistreatment. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[16]

112. The ramifications of Help at Home's failure to keep its patients' Private Information secure are long lasting and severe. Once it is stolen, fraudulent use of such and damage to victims may continue for years.

113. Here, not only was sensitive medical information compromised, but financial information and Social Security numbers were compromised too. The value of both PII and PHI is axiomatic. The value of "big data" in corporate America is astronomical. The fact that identity thieves attempt to steal identities notwithstanding possible heavy prison sentences illustrates beyond a doubt that the Private Information compromised here has considerable market value.

114. PII and PHI are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the dark web for years.

[16] Michael Ollove, "The Rise of Medical Identity Theft in Healthcare," Kaiser Health News, Feb. 7, 2014, *available at*: https://kffhealthnews.org/news/rise-of-indentity-theft/ (last visited on Aug. 21, 2024).

115. As a result, Plaintiff and Class Members are at an increased risk of fraud and identity theft, including medical identity theft, for many years into the future. Thus, Plaintiff and Class Members have no choice but to vigilantly monitor their accounts for many years to come.

CLASS ACTION ALLEGATIONS

116. Plaintiff brings 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 Private Information was compromised in the Data Breach discovered by Help at Home in March 2024, including all those individuals who received notice of the breach.

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

118. Plaintiff reserves the right to amend the class definition.

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

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

121. 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 26,744 members.

122. Typicality. Plaintiff's 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.

123. Adequacy. Plaintiff will fairly and adequately protect the proposed Class's common interests. His interests do not conflict with Class members' interests. And Plaintiff 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.

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

a. if Defendant had a duty to use reasonable care in safeguarding Plaintiff's and the Class's Private Information;

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

c. if Defendant were negligent in maintaining, protecting, and securing Private Information;

d. if Defendant breached contract promises to safeguard Plaintiff and the Class's Private Information;

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 Plaintiff and the Class injuries;

h. what the proper damages measure is; and

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

125. Superiority. A class action will provide substantial benefits and is superior to all other available means for the fair and efficient adjudication of this controversy. The damages or other financial detriment suffered by individual Class members are relatively small compared to the burden and expense that individual litigation against Defendant would require. Thus, it would be practically impossible for Class members, on an individual basis, to obtain effective redress for their injuries. Not only would individualized litigation increase the delay and expense to all parties and the courts, but individualized litigation would also create the danger of inconsistent or contradictory judgments arising from the same set of facts. By contrast, the class action device provides the benefits of adjudication of these issues in a single proceeding, ensures economies of scale, provides comprehensive supervision by a single court, and presents no unusual management difficulties.

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

126. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

127. Plaintiff and the Class entrusted their Private Information to Defendant on the premise and with the understanding that Defendant would safeguard their Private Information, use their Private Information to provide medical services only, and/or not disclose their Private Information to unauthorized third parties.

128. Defendant owed a duty of care to Plaintiff 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 Private Information in a data breach. And here, that foreseeable danger came to pass.

129. Defendant has full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiff and the Class could and would suffer if their Private Information was wrongfully disclosed.

130. Defendant owed these duties to Plaintiff 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 Plaintiff and Class members' Private Information.

131. Defendant owed—to Plaintiff and Class members—at least the following duties to:

a. exercise reasonable care in handling and using the Private Information 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 Plaintiff and Class members within a reasonable timeframe of any breach to the security of their Private Information.

132. Thus, Defendant owed a duty to timely and accurately disclose to Plaintiff and Class members the scope, nature, and occurrence of the Data Breach. After all, this duty is required and necessary for Plaintiff and Class members to take appropriate measures to protect their Private

Information, 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.

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

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

135. Defendant's duty to use reasonable security measures arose because of the special relationship that existed between Defendant and Plaintiff and the Class. That special relationship arose because Plaintiff and the Class (or their third-party agents) entrusted Defendant with their confidential Private Information, a necessary part of obtaining services from Defendant.

136. Under the FTC Act, 15 U.S.C. § 45, Defendant had a duty to use fair and adequate computer systems and data security practices to safeguard Plaintiff and Class members' Private Information.

137. 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 Private Information 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 Plaintiff and the Class members' sensitive Private Information.

138. Pursuant to HIPAA, 42 U.S.C. § 1302(d), *et seq*., Help at Home had a duty to implement reasonable safeguards to protect Plaintiff's and Class Members' Private Information.

139. Specifically, pursuant to HIPAA, Defendant had a duty to render the electronic PHI it maintained unusable, unreadable, or indecipherable to unauthorized individuals by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without the use of a confidential process or key." *See* definition of "encryption" at 45 C.F.R. § 164.304.

140. Defendant violated its duty under Section 5 of the FTC Act and HIPAA by failing to use reasonable measures to protect Private Information and not complying with applicable industry standards as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information 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.

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

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

143. Defendant improperly and inadequately safeguarded the Private Information of Plaintiff and the Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

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

145. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiff's and Class members' Private Information by:

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

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

146. Defendant breached its duties by failing to exercise reasonable care in supervising its agents, contractors, vendors, and suppliers, and in handling and securing the personal information and Private Information of Plaintiff and Class members which actually and proximately caused the Data Breach and Plaintiff and Class members' injury.

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

148. Defendant has admitted that the Private Information of Plaintiff and the Class was wrongfully lost and disclosed to unauthorized third persons because of the Data Breach.

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

150. And, on information and belief, Plaintiff's Private Information has already been published—or will be published imminently—by cybercriminals on the Dark Web.

151. Defendant's breach of its common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiff and Class members actual,

tangible, injury-in-fact and damages, including, without limitation, the theft of their Private Information by criminals, improper disclosure of their Private Information, lost benefit of their bargain, lost value of their Private Information, 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
Breach of Implied Contract
(On Behalf of Plaintiff and the Class)

152. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

153. Plaintiff and Class Members entered into a valid and enforceable contract through which they paid money to Help at Home in exchange for services. That contract included promises by Defendant to secure, safeguard, and not disclose Plaintiff's and Class Members' Private Information.

154. Plaintiff and Class members were required to provide their Private Information to Defendant as a condition of receiving services provided by Defendant. Plaintiff and Class members provided their Private Information to Defendant in exchange for Defendant's services.

155. Plaintiff and Class members reasonably understood that a portion of the funds they paid Defendant would be used to pay for adequate cybersecurity measures.

156. Plaintiff and Class members reasonably understood that Defendant would use adequate cybersecurity measures to protect the Private Information that they were required to provide based on Defendant's duties under state and federal law and its internal policies.

157. Plaintiff and the Class members accepted Defendant's offers by disclosing their Private Information to Defendant or its third-party agents in exchange for services.

158. In turn, and through internal policies, Defendant agreed to protect and not disclose the Private Information to unauthorized persons.

159. In its Privacy Policy, Defendant represented that they had a legal duty to protect Plaintiff's and Class Member's Private Information.

160. Implicit in the parties' agreement was that Defendant would provide Plaintiff and Class members with prompt and adequate notice of all unauthorized access and/or theft of their Private Information.

161. After all, Plaintiff and Class members would not have entrusted their Private Information to Defendant in the absence of such an agreement with Defendant.

162. Plaintiff and the Class fully performed their obligations under the implied contracts with Defendant.

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

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

165. Defendant materially breached the contracts it entered with Plaintiff and Class members (or their third-party agents) by:

a. failing to safeguard their information;

b. failing to notify them promptly of the intrusion into its computer systems that compromised such information.

c. failing to comply with industry standards;

d. failing to comply with the legal obligations necessarily incorporated into the agreements; and

e. failing to ensure the confidentiality and integrity of the electronic Private Information that Defendant created, received, maintained, and transmitted.

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

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

168. And, on information and belief, Plaintiff's Private Information has already been published—or will be published imminently—by cybercriminals on the Dark Web.

169. Plaintiff and Class members performed as required under the relevant agreements, or such performance was waived by Defendant's conduct.

THIRD CAUSE OF ACTION
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

170. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

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

172. Plaintiff and Class members (or their third-party agents) conferred a benefit upon Defendant. After all, Defendant benefitted from (1) using their Private Information to facilitate its business, and (2) from accepting their payment.

173. Defendant appreciated or had knowledge of the benefits it received from Plaintiff and Class members (or their third-party agents).

174. Plaintiff and Class members (or their third-party agents) reasonably understood that Defendant would use adequate cybersecurity measures to protect the Private Information that they were required to provide based on Defendant's duties under state and federal law and its internal policies.

175. Defendant enriched itself by saving the costs they reasonably should have expended on data security measures to secure Plaintiff's and Class members' Private Information.

176. Instead of providing a reasonable level of security, or retention policies, that would have prevented the Data Breach, Defendant instead calculated to avoid its data security obligations at the expense of Plaintiff and Class members by utilizing cheaper, ineffective security measures. Plaintiff and Class members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

177. Under principles of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiff's and Class members' payment because Defendant failed to adequately protect their Private Information.

178. Plaintiff and Class members have no adequate remedy at law.

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

FOURTH CAUSE OF ACTION
Breach of Fiduciary Duty
(On Behalf of Plaintiff and the Class)

180. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

181. Given the relationship between Defendant and Plaintiff and Class members, where Defendant became guardian of Plaintiff's and Class members' Private Information, Defendant

became a fiduciary by its undertaking and guardianship of the Private Information, to act primarily for Plaintiff and Class members, (1) for the safeguarding of Plaintiff and Class members' Private Information; (2) to timely notify Plaintiff and Class members of a Data Breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendant did and does store.

182. 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 Private Information.

183. Because of the highly sensitive nature of the Private Information, Plaintiff and Class members (or their third-party agents) would not have entrusted Defendant, or anyone in Defendant's position, to retain their Private Information had they known the reality of Defendant's inadequate data security practices.

184. Defendant breached its fiduciary duties to Plaintiff and Class members by failing to sufficiently encrypt or otherwise protect Plaintiff's and Class members' Private Information.

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

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

FIFTH CAUSE OF ACTION
Violation of the Illinois Consumer Fraud and Deceptive Business Practices Act
815 ICLS 505/1, *et seq*.
(On Behalf of Plaintiff and the Class)

187. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

188. This claim is brought under the Illinois Consumer Fraud and Deceptive Business Practices Act ("ICFA").

189. Plaintiff and Class members are "consumers" as defined in 815 Ill. Comp. Stat. § 505/1(e).

190. Plaintiff, the Class, and Defendant are "persons" as defined in 815 Ill. Comp. Stat. § 505/1(c).

191. The ICFA applies to Defendant because Defendant engaged in "trade" or "commerce," including the provision of services, as defined under 815 Ill. Comp. Stat. § 505/1(f). Defendant engages in the sale of "merchandise" (including services) as defined by 815 Ill. Comp. Stat. § 505/1(b) and (d).

192. Defendant violated ICFA by, *inter alia*:

a. failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Class members' Private Information, which was a direct and proximate cause of the Data Breach;

b. failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class members' Private Information,

including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq*., which was a direct and proximate cause of the Data Breach;

d. omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Class members' Private Information; and

e. omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq*.

193. Defendant's omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of their Private Information.

194. Defendant intended to mislead Plaintiff and Class members and induce them to rely on its omissions.

195. Had Defendant disclosed to Plaintiff and Class members (or their third-party agents) that its data systems were not secure—and thus vulnerable to attack—Defendant would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Defendant accepted the Private Information that Plaintiff and Class members (or their third-party agents) entrusted to it while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff and Class

members acted reasonably in relying on Defendant's omissions, the truth of which they could not have discovered through reasonable investigation.

196. Defendant acted intentionally, knowingly, maliciously, and recklessly disregarded Plaintiff's and Class members' rights.

197. As a direct and proximate result of Defendant's unfair and deceptive acts and practices, Plaintiff and Class members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

198. And, on information and belief, Plaintiff's Private Information has already been published—or will be published imminently—by cybercriminals on the Dark Web.

199. Plaintiff and Class members seek all monetary and non-monetary relief allowed by law.

200. Defendant's wrongful practices were and are injurious to the public because those practices were part of Defendant's generalized course of conduct that applied to the Class. Plaintiff and the Class have been adversely affected by Defendant's conduct and the public was and is at risk as a result thereof.

201. Defendant also violated 815 ILCS 505/2 by failing to immediately notify Plaintiff and the Class of the nature and extent of the Data Breach pursuant to the Illinois Private Information Protection Act, 815 ILCS 530/1, *et seq*.

202. Pursuant to 815 Ill. Comp. Stat. § 505/10a(a), Plaintiff and the Class seek actual and compensatory damages, injunctive relief, and court costs and attorneys' fees as a result of Defendant's violations of the ICFA.

SIXTH CAUSE OF ACTION
Breach of Confidence
(On Behalf of Plaintiff and the Class)

203. Plaintiff restates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

204. Plaintiff and Class Members have an interest, both equitable and legal, in the Private Information about them that was conveyed to, collected by, and maintained by Help at Home and ultimately accessed and acquired in the Data Breach.

205. As a healthcare provider, Help at Home has a special, fiduciary relationship with its patients, including Plaintiff and Class Members. Because of that special relationship, Help at Home was provided with and stored Plaintiff's and Class Members' Private Information and had a duty to maintain such Information in confidence.

206. Patients like Plaintiff and Class Members have a privacy interest in personal medical and other matters, and Help at Home had a duty not to disclose such matters concerning its patients.

207. As a result of the parties' relationship, Help at Home had possession and knowledge of highly sensitive and confidential PHI and Private Information belonging to Plaintiff and Class Members, information that was not generally known.

208. Plaintiff and Class Members did not consent nor authorize Defendant to release or disclose their Private Information to an unknown criminal actor.

209. Help at Home breached its duty of confidence owed to Plaintiff and Class Members by, among other things: (a) mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of patient information that resulted in the unauthorized access and compromise of Plaintiff's and Class Members' Private Information; (b) mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks; (c) failing to design and implement adequate information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and adjust its information security program in light of the circumstances alleged herein; (f) failing to detect the Breach at the time it began or within a reasonable time thereafter; (g) failing to follow its own privacy policies and practices published to its patients; and (h) making an unauthorized and unjustified disclosure and release of Plaintiff's and Class members' Private Information to a criminal third party.

210. But for Help at Home's wrongful breach of its duty of confidence owed to Plaintiff and Class Members, their Private Information would not have been compromised.

211. As a direct and proximate result of Help at Home's wrongful breach of its duty of confidence, Plaintiff and Class Members have suffered and will continue to suffer the injuries alleged herein.

212. It would be inequitable for Help at Home to retain the benefit of controlling and maintaining Plaintiff's and Class Members' Private Information at the expense of Plaintiff and Class Members.

213. Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, and/or disgorgement or restitution, in an amount to be proven at trial.

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

214. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

215. 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.

216. 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, Plaintiff alleges that Defendant's actions were—and *still* are—inadequate and unreasonable. And Plaintiff and Class members continue to suffer injury from the ongoing threat of fraud and identity theft.

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

d. Defendant breaches of its duties caused—and continues to cause—injuries to Plaintiff and Class members.

218. The Court should also issue corresponding injunctive relief requiring Defendant to use adequate security consistent with industry standards to protect the data entrusted to it.

219. If an injunction is not issued, Plaintiff and the Class will suffer irreparable injury and lack an adequate legal remedy if Defendant experiences a second data breach.

220. And if a second breach occurs, Plaintiff 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 Plaintiff and Class members' injuries.

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

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

PRAYER FOR RELIEF

Plaintiff 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 Plaintiff and the proposed Class, appointing Plaintiff as class representative, and appointing her counsel to represent the Class;

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

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

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

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

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

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

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

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

J. Granting other relief that this Court finds appropriate.

DEMAND FOR JURY TRIAL

Plaintiff demands a jury trial for all claims so triable.

Dated: August 27, 2024

By: */s/ Cassandra Miller*

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

Attorneys for Plaintiff and the Proposed Class