IN THE COURT OF COMMON PLEAS OF PHILADELPHIA COUNTY, PENNSYLVANIA

JOSEPH JONES, individually and on behalf of all others similarly situated,	)	Case No.:
Plaintiff,	)	CLASS ACTION COMPLAINT
v.	)	JURY TRIAL DEMAND
HORIZON HOUSE, INC.,	)	
Defendant.	)	

CLASS ACTION COMPLAINT

Plaintiff Joseph Jones, individually and on behalf of all others similarly situated ("Plaintiff"), brings this action against Defendant Horizon House, Inc. ("Horizon House") to obtain damages, restitution and injunctive relief for the Class, as defined below, from Defendant. Plaintiff makes the following allegations upon information and belief, except as to his own actions, the investigation of his counsel and certain facts that are a matter of public record.

NATURE OF THE ACTION

1. This class action lawsuit arises out of the recent cyberattack and data breach on Horizon House's network that resulted in unauthorized access and exfiltration of highly sensitive and personal patient and employee data (the "Data Breach").

2. As a result of the Data Breach, Plaintiff and approximately 27,823 Class Members suffered present injury and damages in the form of identity theft, the loss of the benefit of their bargain, out-of-pocket expenses and the value of the time reasonably incurred to remedy or mitigate the effects of the unauthorized access, exfiltration, and subsequent criminal misuse of their sensitive and highly personal information.

3. In addition, Plaintiff's and Class Members' sensitive personal information—which was entrusted to Horizon House—was compromised, unlawfully accessed, and exfiltrated by the Data Breach.

4. Information compromised in the Data Breach includes patients' and employees' full names, address, Social Security number, driver's license numbers, state identification number, employment passport number, and medical information (the "Private Information").[1]

5. The healthcare-specific data compromised is protected health information ("PHI") as defined by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), and information such as Plaintiff's Social Security number is deemed personally identifiable information ("PII").

6. Plaintiff brings this class action lawsuit on behalf of those similarly situated to address Defendant's inadequate safeguarding of Class Members' Private Information that they collected and maintained, and for failing to provide timely and adequate notice to Plaintiff and other Class Members that their information had been subject to the unauthorized access of a third party.

7. Defendant maintained the Private Information in a reckless manner. In particular, the Private Information was maintained on Defendant's computer system and network in a condition vulnerable to cyberattacks, including the targeted email phishing attack perpetrated here.

8. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiff's and Class Members' Private Information was a known risk to Defendant, and thus Defendant was on notice that failing to take steps necessary to secure the

[1] https://www.prnewswire.com/news-releases/horizon-house-inc-horizon-house-is-providing-notice-of-a-recent-event-that-may-affect-the-security-of-certain-information-301379756.html (last accessed October 13, 2021).

Private Information from the risk of compromise from a data breach that left that property in a dangerous condition.

9. Plaintiff's and Class Members' identities are now at considerable risk because of Defendant's negligent conduct since the Private Information that Horizon House collected and maintained is now in the hands of data thieves.

10. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes, including but not limited to fraudulently applying for unemployment benefits, 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' health information to target other phishing and hacking intrusions based on their individual health needs, using Class Members' information to obtain government benefits (including unemployment or COVID relief benefits), filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph and providing false information to police during an arrest.

11. As a result of the Data Breach, Plaintiff and Class Members have been exposed to a substantial and present risk of fraud and identity theft. As a result of Defendant's actions and inactions, as set forth herein, Plaintiff and Class Members must now and in the future closely monitor their financial and medical accounts and information to guard against identity theft, among other issues.

12. Plaintiff and Class Members have and may in the future also incur actual monetary costs, including but not limited to the cost of purchasing credit monitoring services, credit freezes, credit reports or other protective measures to deter and detect identity theft.

13. Plaintiff and Class Members may in the future expend time spent mitigating the effects of the Data Breach, including time spent dealing with actual or attempted fraud and identity theft.

14. By his Complaint, Plaintiff seeks to remedy these harms on behalf of himself and all similarly situated individuals whose PII and PHI was accessed during the Data Breach.

15. Plaintiff seeks remedies including, but not limited to, compensatory damages, nominal damages, exemplary damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to Defendant's data security systems, future annual audits and adequate credit monitoring services funded by Defendant.

16. Plaintiff therefore brings this class action lawsuit against Defendant seeking redress for its unlawful conduct and asserting claims for: (i) negligence, (ii) negligence *per se*, (iii) breach of express contract; (iv) breach of implied contract; (v) unjust enrichment; (vi) intrusion into private affairs / invasion of privacy; and (vii) breach of fiduciary duty.

JURISDICTION AND VENUE

17. This Court has jurisdiction over this action and the matters alleged herein.

18. This Court has jurisdiction over Defendant because Defendant is organized under the laws of the Commonwealth of Pennsylvania and the causes of action alleged herein arise from Defendant transacting business in Pennsylvania.

19. Venue is proper in this county pursuant to 231 Pa. Code Rule 1006(a)(1) because Defendant (i) maintains its principal offices and carries on a regular business in this county; and (ii) a substantial part of the events and omissions giving rise to this action occurred in this county.

PARTIES

20. Plaintiff Joseph Jones is currently a resident of the state of Pennsylvania residing in the city of Norristown. Plaintiff Jones had a contract of employment with Horizon House as a Counselor from June 2017 through June 2018. On or about September 17, 2021, Plaintiff Jones received notice from Horizon House about the Data Breach. A copy of the notice is attached hereto as Exhibit A.

21. Defendant Horizon House is a Pennsylvania company with its principal place of business at 120 30th St., Philadelphia, PA, 19104.

DEFENDANT'S BUSINESS

22. Horizon House of Pennsylvania is a non-profit organization providing behavioral health, community-based treatment, employment, education, outpatient, residential treatment, rehabilitation, intellectual and developmental disabilities, homeless, and supported living services in the states of Pennsylvania and Delaware.

23. In the course of and as a condition of servicing its patients, and as a condition of employment with Horizon House, patients and employees (like Plaintiff Jones, a former employee) are required to turn over their PII and PHI to Horizon House, including their full names, Social Security numbers, driver's license numbers, state identification number, employment passport number, and medical information

24. Upon information and belief, Horizon House made promises and representations to its employees, including Plaintiff Jones, that the PII collected from employees as a condition of employment with Horizon House, would be kept safe, confidential, and that the privacy of that information would be maintained.

25. By obtaining, collecting, using and deriving a benefit from Plaintiff's and Class Members' PII and PHI, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' PII and PHI from unauthorized disclosure.

26. Plaintiff and the Class Members have taken reasonable steps to maintain the confidentiality of their PII and PHI.

27. Plaintiff and the Class Members relied on Defendant to keep their PII and PHI confidential and securely maintained, to use this information for business and health purposes only, and to make only authorized disclosures of this information.

THE CYBERATTACK AND DATA BREACH

28. From March 2, 2021, to March 5, 2021, unauthorized individuals gained access to Horizon House's technology system and exfiltrated employee and patient PII and PHI.

29. On March 5, 2021, Horizon House discovered suspicious activity in its technology system and became aware that its system had been breached.

30. Despite becoming aware of the Data Breach as early as March 5, 2021, Horizon House claims it did not discover until nearly six months later that the compromised data contained unencrypted PII and PHI of its patients and employees.

31. This discovery was allegedly made after an investigation was conducted by Horizon House.

32. The investigation revealed that approximately 27,823 individuals were victims of the Data Breach.[2]

[2] *See* https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last accessed October 13, 2021).

33. The investigation further revealed that information accessed by the hackers included: full name, address, Social Security number, driver's license numbers, state identification number, employment passport number, and medical information.[3]

34. Despite discovering the Data Breach as early as March 5, 2021, Defendant did not begin to notify affected individuals (including Plaintiff) of this Data Breach until September 17, 2021, *more than six months after discovering the data breach*, when Horizon House began notifying its patients, states' attorney generals, and the US Department of Health and Human Services.

35. The Data Breach remains under investigation by the U.S. Department of Health and Human Services' Office for Civil Rights.

36. Plaintiff's and Class Members' Private Information was accessed and stolen in the Data Breach, and that information will likely be used for identity theft and fraud.

37. Plaintiff further believes his PII, and that of Class Members, was subsequently sold on the dark web following the Data Breach, as that is the typical *modus operandi* of cybercriminals that commit phishing attacks of this type.

The Data Breach Was Entirely Foreseeable

38. Defendant had obligations created by HIPAA, the employer-employee relationship, contract, industry standards, common law, and its own promises and representations made to Plaintiff and Class Members to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

[3] https://www.prnewswire.com/news-releases/horizon-house-inc-horizon-house-is-providing-notice-of-a-recent-event-that-may-affect-the-security-of-certain-information-301379756.html (last accessed October 13, 2021).

39. Plaintiff and Class Members provided their Private Information to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

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

41. Data breaches, including those perpetrated against the healthcare sector of the economy, have become extremely widespread.

42. In 2019, a record 1,473 data breaches occurred, resulting in approximately 164,683,455 sensitive records being exposed, a 17% increase from 2018.[4]

43. Of the 1,473 recorded data breaches, 525 of them, or 35.64%, were in the medical or healthcare industry.[5]

44. Defendant was aware of the risk of data breaches because such breaches have dominated the headlines in recent years. For instance, the 525 reported breaches reported in 2019 exposed nearly 40 million sensitive records (39,378,157), compared to only 369 breaches that exposed just over 10 million sensitive records (10,632,600) in 2018.[6]

---

[4] *See* https://www.idtheftcenter.org/wp-content/uploads/2020/01/01.28.2020_ITRC_2019-End-of-Year-Data-Breach-Report_FINAL_Highres-Appendix.pdf (last visited Sept. 2, 2021).

[5] *Id.*

[6] *Id.* at 15.

45. In light of recent high profile data breaches at other healthcare partner and provider companies, including, American Medical Collection Agency (25 million patients, March 2019) University of Washington Medicine (974,000 patients, December 2018), Florida Orthopedic Institute (640,000 patients, July 2020), Wolverine Solutions Group (600,000 patients, September 2018), Oregon Department of Human Services (645,000 patients, March 2019), Elite Emergency Physicians (550,000 patients, June 2020), Magellan Health (365,000 patients, April 2020), BJC Health System (286,876 patients, March 2020), Defendant knew or should have known that their electronic health records would be targeted by cybercriminals.

46. 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 prepared for, a potential attack.

47. In fact, according to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in the past year.[7]

48. In 2021 alone there have been over 220 data breach incidents. These approximately 220 data breach incidents have impacted nearly 15 million individuals.

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

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

---

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

51. 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."[8]

52. According to the 2019 Health Information Management Systems Society, Inc. ("HIMMS") Cybersecurity Survey, "[a] pattern of cybersecurity threats and experiences is discernable across U.S. healthcare organizations. Significant security incidents are a near-universal experience in U.S. healthcare organizations with many of the incidents initiated by bad actors, leveraging e-mailas a means to compromise the integrity of their targets."[9]

53. 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]

54. PII and PHI is of great value to hackers and cybercriminals, and the data compromised in the Data Breach can be used in a variety of unlawful manners.

55. PII and PHI can be used to distinguish, identify or trace an individual's identity, such as their name, Social Security Number and medical records.

---

[8] https://www.law360.com/consumerprotection/articles/1220974/fbi-secret-service-warn-of-targeted- ransomware?nl_pk=3ed44a08-fcc2-4b6c-89f0-aa0155a8bb51&utm_source=newsletter&utm_medium=email&utm_campaign=consumerprotection (last visited Sept. 2, 2021).

[9] *See* https://www.himss.org/sites/hde/files/d7/u132196/2019_HIMSS_Cybersecurity_Survey_Final_Report.pdf (last visited Sept. 2, 2021).

[10] https://www.chiefhealthcareexecutive.com/view/how-to-safeguard-hospital-data-from-email-spoofing-attacks (last visited Sept. 2, 2021).

56. This can be accomplished alone or in combination with other personal or identifying information that is connected or linked to anindividual, such as their birthdate, birthplace and mother's maiden name.

57. Given the nature of this Data Breach, it is foreseeable that the compromised PII and PHI can be used by hackers and cybercriminals in a variety of different ways.

58. Indeed, the cybercriminals who possess the Class Members' PII and PHI can readily obtain Class Members' tax returns or open fraudulent credit card accounts in the Class Members' names.

59. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including, upon information and good faith belief, Horizon House.

Defendant Fails to Comply with FTC Guidelines

60. 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.

61. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. These 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.[11]

62. 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 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.[12]

63. The FTC further recommends that companies not maintain PII 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.

64. 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.

65. These FTC enforcement actions include actions against healthcare providers like Defendant. *See, e.g., In the Matter of LabMD, Inc., A Corp*, 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's

---

[11] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited June 3, 2021).

[12] *Id.*

data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.")

66. Defendant failed to properly implement basic data security practices.

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

68. Upon information and belief, Defendant was at all times fully aware of its obligation to protect the PII and PHI of its customers. Defendant was also aware of the significant repercussions that would result from its failure to do so.

Defendant Fails to Comply with Industry Standards

69. As noted above, experts studying cyber security routinely identify healthcare providers as being particularly vulnerable to cyberattacks because of the value of the PII and PHI which they collect and maintain.

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

71. Other best cybersecurity practices that are standard in the healthcare industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems;

protection against any possible communication system; training staff regarding critical points. Defendant failed to follow these cybersecurity best practices, including failure to train staff.

72. 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.

73. These foregoing frameworks are existing and applicable industry standards in the healthcare industry, and Defendant failed to comply with these accepted standards thereby opening the door to the cyber incident and causing the data breach.

Defendant's Conduct Violates HIPAA and Evidences Its Insufficient Data Security

74. HIPAA requires covered entities to protect against reasonably anticipated threats to the security of sensitive patient health information.

75. Defendant Horizon House is a "covered entity" under HIPAA. Covered entities must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical and administrative components.

76. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, *et seq*. These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling PII like the data Defendant left unguarded. The HHS subsequently promulgated multiple regulations under authority of the Administrative Simplification provisions of HIPAA. These rules

include 45 C.F.R. § 164.306(a)(1-4); 45 C.F.R. § 164.312(a)(1); 45 C.F.R. § 164.308(a)(1)(i); 45 C.F.R. § 164.308(a)(1)(ii)(D), and 45 C.F.R. § 164.530(b).

77. A Data Breach such as the one Defendant experienced, is considered a breach under the HIPAA Rules because there is an access of PHI not permitted under the HIPAA Privacy Rule:

> A breach under the HIPAA Rules is defined as, "...the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI."

78. Defendant's Data Breach resulted from a combination of insufficiencies that demonstrate Horizon House failed to comply with safeguards mandated by HIPAA regulations.

Defendant's Breach

79. Defendant breached its obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data.

80. Defendant's unlawful conduct also includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Failing to adequately protect patients' PHI and other private information;

c. Failing to properly monitor its own data security systems for existing intrusions, brute-force attempts and clearing of event logs;

d. Failing to apply all available security updates;

e. Failing to install the latest software patches, update its firewalls, check user account privileges, or ensure proper security practices;

f. Failing to practice the principle of least-privilege and maintain credential hygiene;

g. Failing to avoid the use of domain-wide, admin-level service accounts;

h. Failing to employ or enforce the use of strong randomized, just-in- time local administrator passwords;

i. Failing to properly train and supervise employees in the proper handling of inbound emails;

j. Failing to ensure the confidentiality and integrity of electronic PHI it created, received, maintained and/or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

k. 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);

l. 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)(i);

m. Failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

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

o. Failing to protect against reasonably anticipated uses or disclosuresof electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of45 C.F.R. § 164.306(a)(3);

p. Failing to ensure compliance with HIPAA security standard rules byits workforces in violation of 45 C.F.R. § 164.306(a)(4);

q. Failing to train all members of its workforces effectively on the policies and procedures regarding PHI as necessary and appropriate for the members of its workforces to carry out their functions and tomaintain security of PHI, in violation of 45 C.F.R. § 164.530(b); and/or

r. Failing to render the electronic PHI it maintained unusable, unreadable, or indecipherable to unauthorized individuals, as it had not encrypted the electronic PHI as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key," 45 CFR § 164.304 (definition of encryption).

81. As the result of allowing its computer systems to fall into dire need of security upgrading and its inadequate procedures for handling cybersecurity threats, Defendant negligently and unlawfully failed to safeguard Plaintiff's and the Class Members' Private Information.

82. Accordingly, as outlined below, Plaintiff and Class Members now face a substantial, increased, and immediate risk of fraud and identity theft. In addition, Plaintiff and the Class Members also lost the benefit of the bargain they made with Defendant because of its inadequate data security practices for which they gave good and valuable consideration.

Cyberattacks and Data Breaches Cause Disruption and Put Consumers at a Present Risk of Fraud and Identity Theft

83. Cyberattacks and data breaches at healthcare providers like Defendant are especially problematic because they can negatively impact the overall daily lives of individuals affected by the attack.

84. Researchers have found that among medical service providers that experience a data security incident, the death rate among patients increased in the months and years after the attack.[13]

85. Researchers have further found that at medical service providers that experienced a data security incident, the incident was associated with deterioration in timeliness and patient outcomes, generally.[14]

86. The United States Government Accountability Office released a report in 2007

---

[13] *See* Nsikan Akpan, *Ransomware and Data Breaches Linked to Uptick in Fatal Heart Attacks*, PBS (Oct. 24, 2019), https://www.pbs.org/newshour/science/ransomware-and-other-data-breaches-linked-to-uptick-in-fatal-heart-attacks.

[14] *See* Sung J. Choi, *et al*., *Data Breach Remediation Efforts and Their Implications for Hospital Quality*, 54 Health Services Research 971, 971-980 (2019). Available at https://onlinelibrary.wiley.com/doi/full/10.1111/1475-6773.13203.

regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[15]

87. That is because any victim of a data breach is exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal personally identifiable 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, take over victims' identities in order to engage in illegal financial transactions under the victims' names.

88. 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 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.

89. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit and correcting their credit

[15] *See* U.S. Gov. Accounting Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (2007). Available at https://www.gao.gov/new.items/d07737.pdf.

reports.[16]

90. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud and bank/finance fraud.

91. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits or file a fraudulent tax return using the victim's information.

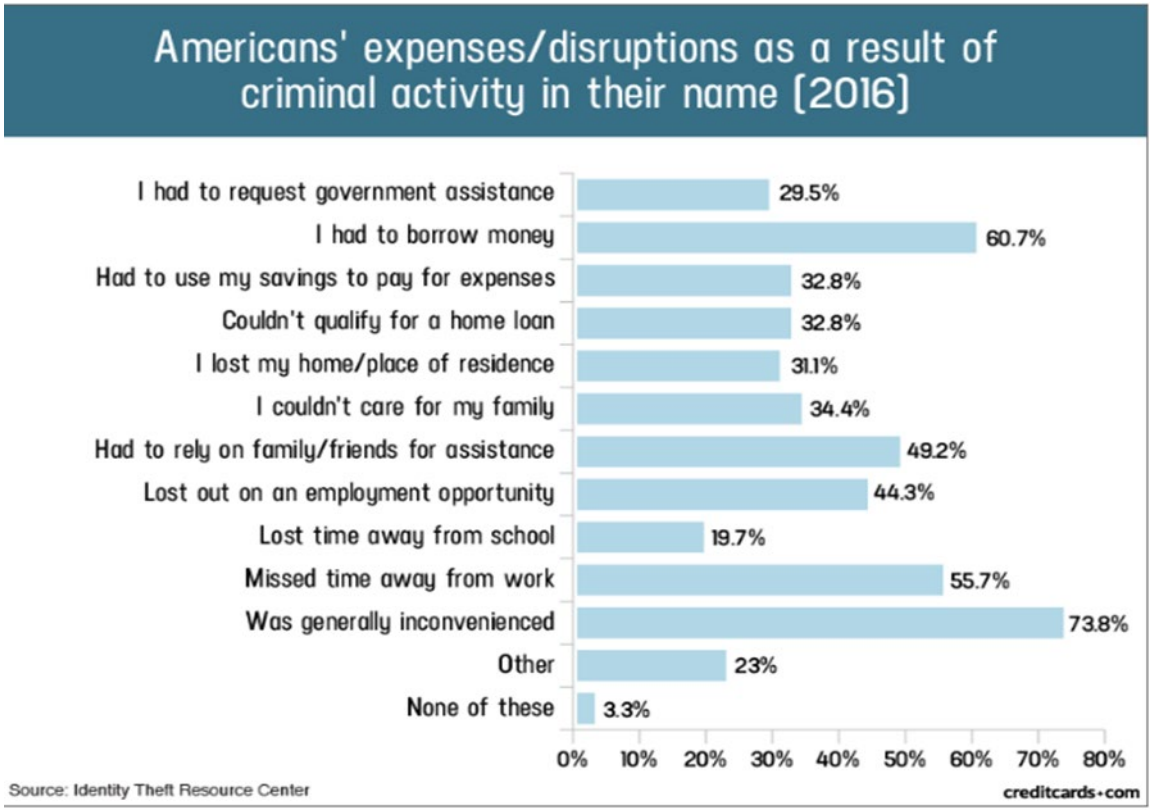
92. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

93. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:[17]

---

[16] *See IdentityTheft.gov*, Federal Trade Commission, https://www.identitytheft.gov/Steps (last visited June 3, 2021).

[17] *See* Jason Steele, *Credit Card and ID Theft Statistics*, CreditCards.com (Oct. 23, 2020) https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php.



94. Moreover, theft of Private Information is gravely serious; PII and PHI is an extremely valuable property right.[18]

95. Its value is axiomatic, considering the value of "big data" in corporate America and the fact that the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

96. Theft of PHI, in particular, is gravely serious: "[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment,

[18] *See, e.g.*, John T. Soma, *et al*, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

insurance and payment records, and credit report may be affected."[19]

97. Drug manufacturers, medical device manufacturers, pharmacies, hospitals and other healthcare service providers often purchase PII and PHI on the black market for the purpose of target marketing their products and services to the physical maladies of the data breach victims themselves. Insurance companies purchase and use wrongfully disclosed PHI to adjust their insureds' medical insurance premiums.

98. Compounding issues for data breach victims is the fact that there may be a substantial time lag – measured in years -- between when harm occurs and when it is discovered and also between when Private Information and/or financial information is stolen and when it is used.

99. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

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

See GAO Report, at 29.

100. Private Information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

101. There is a strong probability that entire batches of stolen information have been dumped on the black market and are yet to be dumped on the black market, meaning Plaintiff and

[19] *See* Federal Trade Commission, *Medical Identity Theft*, http://www.consumer.ftc.gov/articles/0171-medical-identity-theft (last visited June 3, 2021).

Class Members are at a substantial and present risk of fraud and identity theft for many years into the future.

102. Thus, Plaintiff and Class Members must vigilantly monitor their financial and medical accounts for many years to come.

103. Sensitive Private Information can sell for as much as $363 per record according to the Infosec Institute.[20]

104. PII is particularly valuable because criminals can use it to target victims with frauds and scams. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

105. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.[21] Such fraud may go undetected until debt collection calls commence months, or even years, later.

106. Stolen Social Security Numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.[22]

107. Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

108. Moreover, it is not an easy task to change or cancel a stolen Social Security number.

---

[20] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/.

[21] *Identity Theft and Your Social Security Number*, Social Security Administration (2018) at 1. Available at https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited June 3, 2021).

[22] *Id.* at 4.

109. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[23]

110. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[24]

111. Driver's license numbers are also incredibly valuable. "Hackers harvest license numbers because they're a very valuable piece of information. A driver's license can be a critical part of a fraudulent, synthetic identity – which go for about $1200 on the Dark Web. On its own, a forged license can sell for around $200."[25]

112. According to national credit bureau Experian:

> A driver's license is an identity thief's paradise. With that one card, someone knows your birthdate, address, and even your height, eye color, and signature. If someone gets your driver's license number, it is also concerning because it's connected to your vehicle registration and insurance policies, as well as records on file with the Department of Motor Vehicles, place of employment (that keep a copy of your driver's license on file), doctor's office, government agencies, and other entities. Having access to that one number can provide an identity thief with several pieces of information they want to know about you. Next to your Social Security number, your driver's license number is one of the most

---

[23] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft.

[24] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Computer World (Feb. 6, 2015), http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html.

[25] https://www.forbes.com/sites/leemathews/2021/04/20/hackers-stole-customers-license-numbers-from-geico-in-months-long-breach/?sh=3e4755c38658 (last accessed July 20, 2021)

important pieces of information to keep safe from thieves.[26]

113. According to cybersecurity specialty publication CPO Magazine, "[t]o those unfamiliar with the world of fraud, driver's license numbers might seem like a relatively harmless piece of information to lose if it happens in isolation."[27] However, this is not the case. As cybersecurity experts point out:

> "It's a gold mine for hackers. With a driver's license number, bad actors can manufacture fake IDs, slotting in the number for any form that requires ID verification, or use the information to craft curated social engineering phishing attacks."[28]

114. Victims of driver's license number theft also often suffer unemployment benefit fraud, as described in a recent New York Times article.[29]

115. Medical information is especially valuable to identity thieves.

116. According to account monitoring company LogDog, medical data was selling for $50 and up on the dark web.[30]

117. Because of the value of its collected and stored data, the medical industry has experienced disproportionally higher numbers of data theft events than other industries.

---

[26] Sue Poremba, *What Should I Do If My Driver's License Number is Stolen?"* (October 24, 2018) https://www.experian.com/blogs/ask-experian/what-should-i-do-if-my-drivers-license-number-is-stolen/ (last accessed July 20, 2021)

[27] https://www.cpomagazine.com/cyber-security/geico-data-breach-leaks-drivers-license-numbers-advises-customers-to-watch-out-for-fraudulent-unemployment-claims/ (last accessed July 20, 2021)

[28] *Id.*

[29] *How Identity Thieves Took My Wife for a Ride,* NY Times, April 27, 2021 https://www.nytimes.com/2021/04/27/your-money/identity-theft-auto-insurance.html (last accessed July 20, 2021)

[30] Lisa Vaas, *Ransomware Attacks Paralyze, and Sometimes Crush, Hospitals*, Naked Security (Oct. 3, 2019), https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/#content (last accessed July 20, 2021)

118. For this reason, Defendant knew or should have known about these dangers and strengthened its data and email handling systems accordingly. Defendant was put on notice of the substantial and foreseeable risk of harm from a data breach, yet Horizon House failed to properly prepare for that risk.

Plaintiff's and Class Members' Damages

119. To date, Defendant has done little to nothing to provide Plaintiff and the Class Members with relief for the damages they have suffered as a result of the Data Breach.

120. Defendant has merely offered Plaintiff and Class Members credit monitoring services, but this does nothing to compensate them for damages incurred and time spent dealing with the Data Breach.[31] Moreover, the fraud and identity monitoring service offered by Defendant are wholly inadequate as the services are offered for an inadequate length of time and the burden is placed squarely on Plaintiff and Class Members by requiring them to expend time signing up for that service, as opposed to automatically enrolling all victims of this cybercrime.

121. Plaintiff and Class Members have been injured and damaged by the Data Breach.

122. Plaintiff is a former employee of Defendant.

123. Plaintiff typically takes measures to protect his Private Information, and is very careful about sharing his Private Information. He has never knowingly transmitted unencrypted PII or PHI over the internet or any other unsecured source.

124. Plaintiff stores any documents containing his Private Information in a safe and secure location. Moreover, he diligently chooses unique usernames and passwords for his online accounts.

---

[31] *See* Ex. A, Notice Letter at 2 (stating that "[b]ecause it is possible that your Social Security number or financial account information may have been involved, we have arranged to offer you credit monitoring and identity restoration services for a period of 12 months, at no cost to you through an identity and privacy protection company named IDX").

125. To the best of his knowledge, Plaintiff's Private Information was never compromised in any other data breach.

126. Plaintiff's and Class Members' names, addresses, dates of birth, Social Security Numbers, medical diagnosis, insurance information and other protected health information were all compromised in the Data Breach and are now in the hands of the cybercriminals who accessed Defendant's computer system.

127. After and as a result of the Data Breach, Plaintiff Jones has experienced a substantial increase in suspicious scam phone calls, emails, texts, all of which appear to be placed with the intent to obtain personal information to commit identity theft by way of a social engineering attack.

128. Since being notified of the Data Breach on or about September 17, 2021, Plaintiff Jones has spent time monitoring his confidential accounts for fraud and dealing with the impact of the Data Breach, valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time included time spent on the telephone and sorting through his unsolicited texts, verifying the legitimacy of the Data Breach, exploring credit monitoring and identity theft insurance options, and self-monitoring his accounts. This time has been lost forever and cannot be recaptured.

129. Due to the Data Breach, Plaintiff Jones anticipates spending considerable additional amounts of time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

130. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been placed at a substantial and present risk of harm from fraud and identity theft.

131. As a direct and proximate result of Defendant's conduct, Plaintiff and Class

Members have been forced to expend time dealing with the effects of the Data Breach.

132. Plaintiff and Class Members face substantial risk of out-of-pocket fraud losses such as unemployment benefits unlawfully applied for, loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud and similar identity theft.

133. Plaintiff and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their Private Information as potential fraudsters could use that information to more effectively target such schemes to Plaintiff and Class Members.

134. Plaintiff and Class Members may also incur additional out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees and similar costs directly or indirectly related to the Data Breach.

135. Plaintiff and Class Members also suffered a loss of value of their Private Information when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases.

136. Plaintiff and Class Members were also damaged via benefit-of-the-bargain damages. Plaintiff and other employee and former employee Class Members provided their labor to Defendant in exchange for a contractual agreement to protect their PII. Patient Class Members overpaid for medical devices in a transaction that was intended to be accompanied by adequate data security but was not. Part of the price Patient Class Members paid to Defendant was intended to be used by Defendant to fund adequate security of Horizon House's computer property and Patient Class Members' PII and PHI. Thus, Plaintiff and the Class Members did not get what they bargained for, paid for and agreed to.

137. Plaintiff and Class Members will spend significant amounts of time mitigating the effect of attempted fraud and identity theft, including:

a. Reviewing and monitoring sensitive accounts and finding fraudulent insurance claims, loans, and/or government benefits claims;

b. Purchasing credit monitoring and identity theft prevention;

c. Placing "freezes" and "alerts" with reporting agencies;

d. Spending time on the phone with or at financial institutions, healthcare providers, and/or government agencies to dispute unauthorized and fraudulent activity in their name;

e. Contacting financial institutions and closing or modifying financial accounts; and,

f. Closely reviewing and monitoring Social Security Number, medical insurance accounts, bank accounts, and credit reports for unauthorized activity for years to come.

138. Moreover, Plaintiff and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing Private Information is not accessible online and that access to such data is password protected.

139. Further, as a result of Defendant's conduct, Plaintiff and Class Members are forced to live with the anxiety that their Private Information—which contains the most intimate details about a person's life, including what ailments they suffer, whether physical or mental—may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any

right to privacy whatsoever.

140. As a direct and proximate result of Defendant's actions and inactions, Plaintiff and Class Members have suffered anxiety, emotional distress, and loss of privacy, and are at an increased risk of future harm.

CLASS ACTION ALLEGATIONS

141. Plaintiff brings this action on behalf of himself and on behalf of all other persons similarly situated.

142. Plaintiff proposes the following Class definitions, subject to amendment as appropriate:

> All persons Horizon House identified as being among those individuals impacted by the Data Breach, including all who were sent a notice of the Data Breach (the "Class").
>
> All employees of Horizon House identified as being among those individuals impacted by the Data Breach, including all who were sent a notice of the Data Breach (the "Employee Subclass").

143. Excluded from the Classes are Defendant's officers, directors, and employees; any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Classes are members of the judiciary to whom this case is assigned, their families and Members of their staff.

144. Numerosity. The Members of the Classes are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time, based on information and belief, the Classes consist of approximately 27,823 patients, employees, and former employees of Horizon House whose PII and PHI was compromised in Data Breach.

145. Commonality. There are questions of law and fact common to the Classes, which

predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' PII and PHI;

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

c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations including, *e.g.*, HIPAA and the FTC Act;

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

e. Whether this phishing cyberattack against a healthcare entity like Defendant was reasonably foreseeable;

f. Whether Defendant owed a duty to Plaintiff and Class Members to safeguard their Private Information;

g. Whether Defendant breached its duty to Plaintiff and Class Members to safeguard their Private Information;

h. Whether Defendant knew or should have known that its training, email handling procedures and processes, data security systems and monitoring processes were deficient;

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

j. Whether Plaintiff and Class Members suffered damages as a result of Defendant's misconduct;

k. Whether Defendant's conduct was negligent;

l. Whether Defendant violated the consumer protection statute invoked below;

m. Whether Defendant breach implied contracts with Plaintiff and Class Members;

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

o. Whether Defendant failed to provide notice of the Data Breach in a timely manner, and;

p. Whether Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages, treble damages, and/or injunctive relief.

146. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's private information, like that of every other Class Member, was compromised in the Data Breach.

147. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of the Members of the Classes, and has no interest antagonistic to the Classes. Plaintiff's Counsel are competent and experienced in litigating Class actions.

148. Predominance. Defendant have engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff's and Class Members' data was stored on the same computer system (Defendant's employee email accounts) and unlawfully accessed in the

same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

149. Superiority. A Class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a Class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

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

CAUSES OF ACTION

FIRST COUNT
NEGLIGENCE
(On Behalf of Plaintiff and the Class)

151. Plaintiff re-alleges and incorporates by reference Paragraphs 1 through 150 above as if fully set forth herein.

152. Defendant required its employees and patients, including Plaintiff and Class Members, to submit non-public Private Information in the ordinary course of providing

employment or medical services.

153. By collecting and storing this data in its computer property, and sharing it and using it for commercial gain, Defendant owed a duty of care to use reasonable means to secure and safeguard its computer property—and Class Members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from unauthorized access and exfiltration.

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

155. Defendant owed a duty of care to Plaintiff and Class Members to provide data security that would protect against reasonably foreseeable risks, that was consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks (and the personnel responsible for them) adequately protected Plaintiff's and Class Members' PII and PHI.

156. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and its employees and patients, which is recognized by laws and regulations including but not limited to HIPAA, as well as common law.

157. Defendant was in a superior position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

158. Defendant's duty to use reasonable security measures under HIPAA required Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1).

159. Some or all of the medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

160. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

161. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential PII and PHI.

162. Furthermore, by requiring customers and employees to provide their Private Information, Defendant assumed a legal duty to exercise reasonable care in handling and/or storing that Private Information.

163. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Plaintiff's and Class Members' PII and PHI. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. failing to implement multifactor authentication prior to the email phishing attack;

b. failing to adequately train its employees on the risks of malicious emails;

c. failing to adequately train its employees on the proper handling of suspicious emails

d. failing to implement appropriate technical safeguards on its email system.

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

f. Failing to adequately monitor the security of their networks and systems;

g. Failing to ensure that their email system had plans in place to maintain reasonable data security safeguards;

h. Failing to have in place mitigation policies and procedures;

i. Allowing unauthorized access to Class Members' Private Information;

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

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

164. It was foreseeable that Defendant's failure to use reasonable measures to protect Plaintiff's and Class Members' PII and PHI would result in injury to Plaintiff and Class Members.

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

166. It was therefore foreseeable that the failure to adequately safeguard Plaintiff's and Class Members' PII and PHI would result in one or more types of injuries to Plaintiff and Class Members.

167. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

168. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, *e.g.,* (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures and (iii) continue to provide adequate credit monitoring to all Class Members.

SECOND COUNT
NEGLIGENCE *PER SE*
(On Behalf of Plaintiff and the Class)

169. Plaintiff repeats and re-alleges each and every allegation contained in Paragraphs 1 through 150 as if fully set forth herein.

170. 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's, of failing to use reasonable measures to protect Private Information. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

171. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and PHI and not complying with applicable industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of PII and PHI it obtained and stored, and the foreseeable consequences of the Data Breach for companies of Defendant's magnitude, including, specifically, the immense damages that would result to Plaintiff and Members of the Class due to the valuable nature of the PII and PHI at issue in this case—including Social Security numbers.

172. Defendant's violations of Section 5 of the FTC Act constitute negligence *per se*.

173. Plaintiff and members of the Class are within the class of persons that the FTC Act was intended to protect.

174. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of its failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and members of the Class.

175. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and members Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft and attempted fraud; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) 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 tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of its current and former employees and customers in its continued possession; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and members of the Class.

176. Additionally, as a direct and proximate result of Defendant's negligence *per se*, Plaintiff and members of the Class have suffered and will suffer the continued risks of exposure of their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in their continued possession.

THIRD COUNT
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Class)

177. Plaintiff repeats and re-alleges each and every allegation contained in Paragraphs 1 through 150 as if fully set forth herein.

178. When Plaintiff and Class Members provided their PII and PHI to Horizon House in exchange for medical services from Defendant or an employment relationship with Defendant, they entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such information.

179. Defendant solicited and invited Class Members to provide their Private Information as part of Defendant's regular business practices.

180. Plaintiff and Class Members accepted Defendant's offers and provided their PII and PHI to Defendant. Defendant accepted the PII and PHI, and there was a meeting of the minds that Defendant would secure, protect, and keep the PII and PHI confidential.

181. In entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations, including HIPAA, and were consistent with industry standards.

182. Class Members who paid money to Defendant reasonably believed and expected that Defendant would use part of those funds to obtain adequate data security. Defendant failed to do so.

183. Plaintiff and Class Members who provided their labor to Defendant reasonably believed and expected that Defendant would use part of those funds to obtain adequate data security. Defendant failed to do so.

184. Plaintiff and Class Members would not have entrusted their Private Information to

Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure. Plaintiff and Class Members would not have entrusted their Private Information to Defendant in the absence of its implied promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

185. Plaintiff and Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

186. Defendant breached its implied contracts with Class Members by failing to safeguard and protect their Private Information, in all the ways described in Paragraph 65 above.

187. As a direct and proximate result of Defendant's breaches of the implied contracts, Plaintiff and Class Members sustained damages as alleged herein.

188. Plaintiff and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach, including the loss of the benefit of the bargain.

189. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, *e.g.*, (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

FOURTH COUNT
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Class)

199. Plaintiff repeats and re-alleges each and every allegation contained in Paragraphs 1 through 150 as if fully set forth herein.

200. This count is plead in the alternative to Count Four (breach of implied contract).

201. Plaintiff and Class Members conferred a monetary benefit on Defendant, by

providing Defendant with their valuable PII and PHI.

202. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class Members' PII and PHI.

203. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to avoid their 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.

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

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

206. If Plaintiff and Class Members knew that Defendant had not secured their PII and PHI, they would not have agreed to provide their PII and PHI to Defendant.

207. Plaintiff and Class Members have no adequate remedy at law.

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

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

210. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them.

FIFTH COUNT
INTRUSION INTO PRIVATE AFFAIRS / INVASION OF PRIVACY
(On Behalf of Plaintiff and All Class Members)

211. Plaintiff repeats and re-alleges each and every allegation contained in all Paragraphs 1 through 150 above as if fully set forth herein.

212. The Commonwealth of Pennsylvania recognizes the tort of Intrusion into Private Affairs, and adopts the formulation of that tort found in the Restatement (Second) of Torts, which states:

> One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.

Restatement (Second) of Torts § 652B (1977); *see Vogel v. W.T. Grant Co.*, 458 Pa. 124, 327 A.2d 133 (1974).

213. Plaintiff and Class Members had a reasonable expectation of privacy, and freedom from exposure, in the Private Information Defendant mishandled.

214. Defendant's conduct as alleged above intruded upon Plaintiff's and Class Members' private aspects under common law.

215. Defendant's intrusion was substantial and unreasonable enough to be legally cognizable, in that the reasonable expectation of persons of normal and ordinary sensibilities, including Plaintiff, is that their Private Information disclosed to the providers of their medical care will be securely and confidentially kept.

216. By intentionally failing to keep Plaintiff's and Class Members' Private Information safe, and by intentionally misusing and/or disclosing said information to unauthorized parties for unauthorized use, Defendant intentionally invaded Plaintiff's and Class Members' privacy by intentionally and substantially intruding into Plaintiff's and Class Members' private affairs in a manner that identifies Plaintiff and Class Members and that would be highly offensive and objectionable to an ordinary person.

217. Defendant knew that an ordinary person in Plaintiff's or a Class member's position would consider Defendant's intentional actions highly offensive and objectionable.

218. Defendant invaded Plaintiff's and Class Members' right to privacy and intruded into Plaintiff's and Class Members' private affairs by intentionally misusing and/or disclosing their Private Information without their informed, voluntary, affirmative, and clear consent.

219. As a proximate result of such intentional misuse and disclosures, Plaintiff's and Class Members' reasonable expectations of privacy in their Private Information was unduly frustrated and thwarted. Defendant's conduct amounted to a substantial and serious invasion of Plaintiff's and Class Members' protected privacy interests causing anguish and suffering such that an ordinary person would consider Defendant's intentional actions or inaction highly offensive and objectionable.

220. In failing to protect Plaintiff's and Class Members' Private Information, and in intentionally misusing and/or disclosing their Private Information, Defendant acted with intentional malice and oppression and in conscious disregard of Plaintiff's and Class Members' rights to have such information kept confidential and private. Plaintiff, therefore, seeks an award of damages on behalf of himself and the Class.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all others similarly situated, prays for judgment against Defendant as follows:

a) For an Order certifying this action as a class action and appointing Plaintiff and his counsel to represent the Class;

b) For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' PII and PHI, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;

c) For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage and safety, and to disclose with specificity the type of PII and PHI compromised during the Data Breach;

d) For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

e) Ordering Defendant to pay for not less than three years of credit monitoring services for Plaintiff and the Class;

f) For an award of actual damages, compensatory damages, nominal damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

g) For an award of punitive damages, as allowable by law;

h) For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

i) Pre- and post-judgment interest on any amounts awarded and

j) Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury on all claims so triable.

Dated: October 22, 2021

Respectfully Submitted,

By: /s/ Jonathan M. Jagher

Jonathan M. Jagher
PA I.D. No. 204721
FREED KANNER LONDON & MILLEN LLC
923 Fayette Street
Conshohocken, PA 19428
Tel: 610.234.6486
Fax: 224.632.4521
jjagher@fklmlaw.com

MASON LIETZ & KLINGER LLP
Gary E. Mason (*pro hac vice forthcoming*)
David K. Lietz (*pro hac vice forthcoming*)
5101 Wisconsin Ave., NW, Suite 305
Washington, DC 20016
Phone: 202.640.1160
gmason@masonllp.com
dlietz@masonllp.com

Gary M. Klinger (*pro hac vice forthcoming*)

MASON LIETZ & KLINGER LLP
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Tel.: (202) 975-0477
gklinger@masonllp.com

Attorneys for Plaintiff and
the Proposed Class

ClassAction.org
