Thiago M. Coelho, SBN 324715
thiago@wilshirelawfirm.com
Carolin K. Shining, SBN 201140
cshining@wilshirelawfirm.com
Jonas P. Mann, SBN 263314
jmann@wilshirelawfirm.com
Jennifer M. Leinbach, SBN 281404
jleinbach@wilshirelawfirm.com
Jesenia A. Martinez, SBN 316969
Jesenia.martinez@wilshirelawfirm.com
Jesse S. Chen, SBN 336294
jchen@wilshirelawfirm.com
WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd., 12th Floor
Los Angeles, California 90010
Telephone: (213) 381-9988
Facsimile: (213) 381-9989

Attorneys for Plaintiffs and Proposed Class

UNITED STATES DISTRICT COURT

EASTERN DISTRICT OF CALIFORNIA

CHRISTEN LYNCH, individually, and on behalf of all other similarly situated,

Plaintiffs,

v.

COMMUNITY PSYCHIATRY MANAGEMENT, LLC d/b/a MINDPATH HEALTH, a Delaware Limited Liability Company,

Defendants.

Case No.:

CLASS ACTION

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

CLASS ACTION COMPLAINT

Plaintiff Christen Lynch ("Plaintiff"), individually, and on behalf of all others similarly situated, brings this Class Action Complaint against Defendant Community Psychiatry Management, LLC d/b/a Mindpath Health ("Mindpath" or "Defendant"), based upon personal knowledge as to themselves, their own acts, and as to all other matters upon information and belief, based upon, *inter alia*, the investigations of their attorneys.

NATURE OF THE ACTION

1. On July 5, 2022, Defendant Mindpath discovered that it had experienced a data breach whereby two of its employee email accounts—one in March of 2022 and one in June of 2022—had been subject to unauthorized access. This breach impacted the personal identifying information ("PII") and protected health information ("PHI") of approximately 193,947 of Mindpath's patients. This information included, *inter alia*, the names, addresses, dates of birth, medical diagnosis and treatment information, and Social Security numbers, of those patients.

2. According to its website, Mindpath is a leading, independent provider of outpatient behavioral health services in the United States.[1] As part of its business operations, Mindpath collects and stores the PII and PHI of its patients.

3. Under statute and regulation, Mindpath had a duty to implement reasonable and adequate industry-standard data security policies and safeguards to protect its patient's PII and PHI. However, Defendant failed to implement such security policies and safeguards and allowed third-party hackers to exfiltrate its patients' PII and PHI.

4. Plaintiff and Class Members have suffered injuries and damages. As a result of Defendant's wrongful actions and inactions, Plaintiff and Class Members have suffered injuries and damages. Plaintiff' and Class Members' sensitive PII and PHI, including their Social Security Numbers, have been compromised. Plaintiff and Class Members have had their privacy rights violated and are now exposed to a heightened risk of identity theft and medical fraud for the remainder of their lifetimes. Plaintiff and Class Members must now spend time and money on

[1] https://www.mindpath.com/about/.

prophylactic measures, such as increased monitoring of their personal and financial accounts, and the purchase of credit monitoring services, to protect themselves from future loss. Plaintiff and Class Members have also lost the value of their PII and PHI.

5. Further, Defendant unreasonably delayed in notifying Plaintiff and Class Members of the data breach until approximately January 9, 2023—despite having discovered the breach on or around July 5, 2022, over six months earlier.

6. As a result of Defendant's wrongful actions and inactions, Plaintiff and Class Members have had their PII and PHI compromised and stolen by nefarious third-party hackers, have had their privacy rights violated, have been exposed an increased risk of fraud and identity theft, and have otherwise suffered damages. Plaintiff and Class Members bring this action to seek redress against Defendant.

PARTIES

7. Plaintiff Christen Lynch is a citizen of the State of North Carolina who resides in Winston Salem, North Carolina. Plaintiff Lynch is a former patient of Defendant who received healthcare services from Defendant. As a requirement in receiving those services, Plaintiff Lynch provided Defendant with her PII and PHI. On January 9, 2023, Plaintiff was notified by Defendant that her PII and PHI had been impacted by the data breach.

8. Defendant Community Psychiatry Management, LLC d/ba/ Mindpath Health is a Delaware limited liability company with its principal place of business located at 3835 N Freeway Blvd Ste 100, Sacramento, CA 95834. Defendant's registered agent for service of process is the CT Corporation System, who is located at 28 Liberty Street, New York, NY 10005. Defendant also maintains several CA Registered Corporate Agents, all of whom are located at 330 N Brand Blvd., Glendale, CA 91203.

JURISDICTION AND VENUE

9. This Court has subject matter jurisdiction over the claims asserted herein pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2) because Plaintiff and other members of the putative class are citizens of States different from Defendant and the amount in controversy in this action exceeds $5 million.

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

10. This Court also has personal jurisdiction over the Parties because Defendant resides in and routinely conducts business in this District and has sufficient minimum contacts in this District to have intentionally availed themselves to this jurisdiction.

11. Venue is proper in this District because, among other things: (a) Defendant resides in and conducts substantial business in this District; (b) Defendant directed its services at residents in this District, and (c) many of the acts and omissions that gave rise to this action took place in this District.

FACTUAL ALLEGATIONS

A. The Data Breach

12. Defendant Mindpath is a HIPAA healthcare provider that provides outpatient behavioral services to patients in the States of Arizona, California, Florida, Minnesota, North Carolina, Ohio, South Carolina, and Texas. In providing these services, Defendant requires that its patients provide them with their PII and PHI, which it collects and stores in its data servers. As a result, Defendant's internal systems store the PII and PHI of hundreds of thousands of its patients throughout the United States.

13. In March of 2022, and again in June of 2022, Defendant's employee emails were compromised by unauthorized third-party hackers. As a result, those hackers accessed and obtained Plaintiff's and Class Members' sensitive PII and PHI—including, but not limited to, their names, addresses, dates of birth, medical diagnosis and treatment information, and Social Security numbers. In its data breach report filed with the United States Secretary of Health and Human Services, Defendant reported that the data breach had affected 193,947 individuals.[2]

B. Defendant's Unreasonable and Inadequate Data Security

14. Plaintiff and Class Members provided their sensitive PII and PHI to Defendant with the reasonable expectation and mutual understanding that Defendant would implement reasonable and adequate cybersecurity safeguards to protect their PII and PHI from unauthorized disclosure.

[2] "Cases Currently Under Investigation" U.S. Department of Health and Human Services Offices for Civil Rights https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf. (last accessed February 8, 2023).

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

What Plaintiff and Class Members did not expect was that Defendant would cause their sensitive PII and PHI to be obtained by unauthorized third parties by leaving its employee email accounts, which contained patient PII/PHI, vulnerable to unauthorized third-party access.

15. Defendant's employee email accounts were likely compromised by ransomware. Ransomware is a form of malware designed to gain unauthorized access to and encrypt files on a device or server, rendering any files and the systems that rely on them unusable. Malicious actors use ransomware to unlawfully obtain private, sensitive and/or confidential information, and then demand a ransom in exchange for decrypting the affected files. Ransomware attacks are often targeted towards businesses such as Defendant that are known to collect and store the confidential and sensitive PII/PHI of hundreds of thousands of individuals.

16. Ransomware attacks are highly preventable through the implementation of reasonable and adequate cybersecurity safeguards and/or proper employee cybersecurity training, as the vast majority of ransomware incidents are caused by poor user practices, lack of cybersecurity training, and weak passwords or access management.[3] For instance, ransomware is most commonly spread through "phishing" emails sent to employees with customer or patient data on their devices, which contain malicious attachments that allow a hacker to access that patient data. Ransomware is also commonly spread when an employee visits an infected website on a device connected to a company server. As such, businesses with adequate and reasonable data security practices train their employees not to open email attachments from unrecognized emails or visit unauthorized websites on company device.

17. Defendant clearly recognized its duty to implement adequate and reasonable security measures, such as those described above and others, in its HIPAA Notice of Privacy Practices, wherein it states "[w]e understand the importance of privacy and are committed to maintaining the confidentiality of your medical information," and that "[w]e are required by law

[3] "Most common delivery methods and cybersecurity vulnerabilities causing ransomware infections according to MSPs worldwide as of 2020." Statista, https://www.statista.com/statistics/700965/leading-cause-of-ransomware-infection/ (last accessed February 8, 2023).

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

to maintain the privacy of protected health information."[4] However, Defendant clearly failed to implement such adequate and reasonable cybersecurity safeguards to protect Plaintiff and Class Members' PII and PHI. As a result, Plaintiff and Class Members' PII and PHI was breached.

C. Defendant's Unreasonably Delayed Data Breach Notification

18. Defendant owed Plaintiff and Class Members a duty under state law and federal law to provide timely notification of the data breach. Under N.C. Gen. Stat. §§75-65(a), Defendant was required to provide affected persons such as Plaintiffs and Class Members notification of their data breach "without unreasonable delay."

19. Likewise, 45 C.F.R. §164.404 of the Health Insurance Portability and Accountability Act ("HIPAA") provides that a "covered entity shall provide the notification required by paragraph (a) of this section without unreasonable delay and in no case later than 60 calendar days after discovery of a breach." As a healthcare provider, Defendant is a covered entity under HIPAA.

20. Defendant discovered the data breach on or around July 5, 2022. Despite this, Defendant did not disclose the data breach and provide notice to affected patients until on or around January 9, 2023—over six months later. Defendant did not and has not provided any reason or justification for this unreasonable delay in notification. As a result of Defendant's delay, Plaintiff and Class Members were left unaware that their sensitive PII and PHI had been acquired by nefarious third-party hackers for far longer than they should have been and were thus unreasonably delayed in their ability and opportunity to take emergency prophylactic measures to protect their personal and financial accounts.

D. Defendant's Obligation to Protect Patient PII/PHI Under Federal Law

21. As a HIPAA covered entity, Defendant holds a statutory duty under HIPAA and other federal and state statutes to safeguard Plaintiff's and Class Member's PII/PHI. Under the HIPAA Privacy Rule, Defendant is required to, *inter alia*:

[4] "Health Insurance Portability & Accountability Act (HIPAA) Notice of Privacy Practices" https://www.mindpath.com/hipaa-privacy-practices/ (last accessed February 8, 2023).

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

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

b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and

d. Ensure compliance with the above data security procedures by their workforce.

45 CFR §164. 306(a)

22. The HIPAA Privacy Rule also requires Defendant to "review and modify the security measures implemented…as needed to continue provision of reasonable and appropriate protection of electronic protected health information" under 45 C.F.R. §164.306(e) and to "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights" under 45 C.F.R. §164.312(a)(1).

23. Further, the Federal Trade Commission Act, 15 U.S.C. §45 prohibits businesses such as Defendant from engaging in "unfair or deceptive acts or practices affecting commerce." The Federal Trade Commission ("FTC") has found that a company's failure to maintain reasonable and appropriate data security for the consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236, 243 (3rd Cir. 2015).

24. Defendant has failed to comply with each of these federal statutes by failing to implement and maintain reasonable security procedures to protect Plaintiff and Class Members' PII/PHI.

E. Defendant's Failure to Comply with Industry Data Security Standards and Regulations

25. Experts in the field of data security are in consensus that healthcare providers such as Defendant are specifically targeted by hackers due to the value of the PII/PHI that they collect

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

and maintain as a part of their ordinary course of business. As such, experts have identified several best practices that healthcare providers such as Defendant should implement and follow in order to best protect themselves from unauthorized access.

26. Such best practices are outlined in the National Institute of Standards and Technology's ("NIST") "Security and Privacy Controls for Information Systems and Organizations" publication. These best practices include, *inter alia*, maintaining a plan of action for preventing and addressing data breaches, training and educating employees on data security, implementing strong password requirements, implementing multi-layer security such as two-factor authentication, installation and maintenance of firewalls, anti-virus and anti-malware software, implementing data encryption, monitoring and protection of web browsers and email management systems, and limiting the number of employees with access privileges to patient PII/PHI. *See, e.g*, NIST SP 800-53, Rev. 5 AC-1, AC-2, AC-3, AC-4, AC-5, AC-6, AT-1, AT-3, CA-1, CA-2, CA-3, CA-7, IA-1, IA-2, IA-3, PL-1, PL-2, PM-1, PT-1, PT-2, PT-3.

27. The FTC has also promulgated numerous guides for business which highlight the importance of implementing reasonable data security practices. In 2016, the FTC updated its publication, "Protecting Personal Information: A Guide for Business,"[5] which establishes guidelines for fundamental data security principles and practices for business. Among other things, the guidelines dictate businesses should protect any 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 security problems. The guidelines also recommend that businesses implement an intrusion detection system to expose breaches as soon as they occur; monitor all incoming traffic for activity indicating someone is attempting to infiltrate or hack the system; monitor instances when large amounts of data are transmitted to or from the system; and have a response plan ready in the event

[5] Federal Trade Commission, *Protecting Personal Information: A Guide for Business* (Oct. 2016), https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business. (last accessed February 8, 2023).

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

of a breach.[6] Additionally, the FTC recommends that companies 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.[7]

F. Applicable Standards of Care

28. In addition to their obligations under federal law and regulation, Defendant owed a duty to Plaintiff and the Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII/PHI in their possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendant owed a duty to Plaintiff and the Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that their computer system and networks, and the personnel responsible for them, adequately protected the PII/PHI of Plaintiff and Class Members.

29. Defendant owed a duty to Plaintiff and the Class Members to design, maintain, and test their computer system to ensure that the PII/PHI in Defendants' possession was adequately secured and protected.

30. Defendant owed a duty to Plaintiff and the Class Members to create and implement reasonable data security practices and procedures to protect the PII/PHI in their possession, including adequately training their employees and others who accessed the PII/PHI in their possession, including adequately training their employees and others who accessed PII/PHI in their computer systems on how to adequately protect PII/PHI.

31. Defendant owed a duty of care to Plaintiff and Class Members to implement processes that would detect a breach of their data security systems in a timely manner.

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

---

[6] *Id.*

[7] Federal Trade Commission, *Start With Security: A Guide for Business* (Jun. 2015) https://www.ftc.gov/business-guidance/resources/start-security-guide-business. (last accessed February 8, 2023).

32. Defendant owed a duty to Plaintiff and the Class Members to act upon data security warnings and alerts in a timely fashion.

33. Defendant owed a duty to Plaintiff and Class Members to disclose if their computer systems and data security practices were inadequate to safeguard individuals' PII/PHI from theft because such an inadequacy would be a material fact in the decision to provide or entrust their PII/PHI to Defendant.

34. Defendant owed a duty to Plaintiff and the Class Members to disclose in a timely and accurate manner when the data breach occurred.

35. Defendant owed a duty of care to Plaintiff and the Class Members because they were foreseeable and probable victims of any inadequate data security practices. Defendant received PII/PHI from Plaintiff and Class Members with the understanding that Plaintiff and Class Members expected their PHI/PII to be protected from disclosure. Defendant knew that a breach of its data systems would cause Plaintiff and Class Members to incur damages.

G. Stolen Information is Valuable to Hackers and Thieves

36. It is well known, and the subject of many media reports, that PII/PHI is highly coveted and a frequent target of hackers. Especially in the technology industry, the issue of data security and threats thereto is well known. Despite well-publicized litigation and frequent public announcements of data breaches, Defendant opted to maintain an insufficient and inadequate system to protect the PII/PHI of Plaintiff and Class Members.

37. Plaintiff and Class Members value their PII/PHI, as in today's electronic-centric world, their PII/PHI is required for numerous activities, such as new registrations to websites, or opening a new bank account, as well as signing up for special deals.

38. Legitimate organizations and criminal underground alike recognize the value of PII/PHI. That is why they aggressively seek and pay for it.

39. PII/PHI is highly valuable to hackers. Identity thieves use stolen PII for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud. PII that is

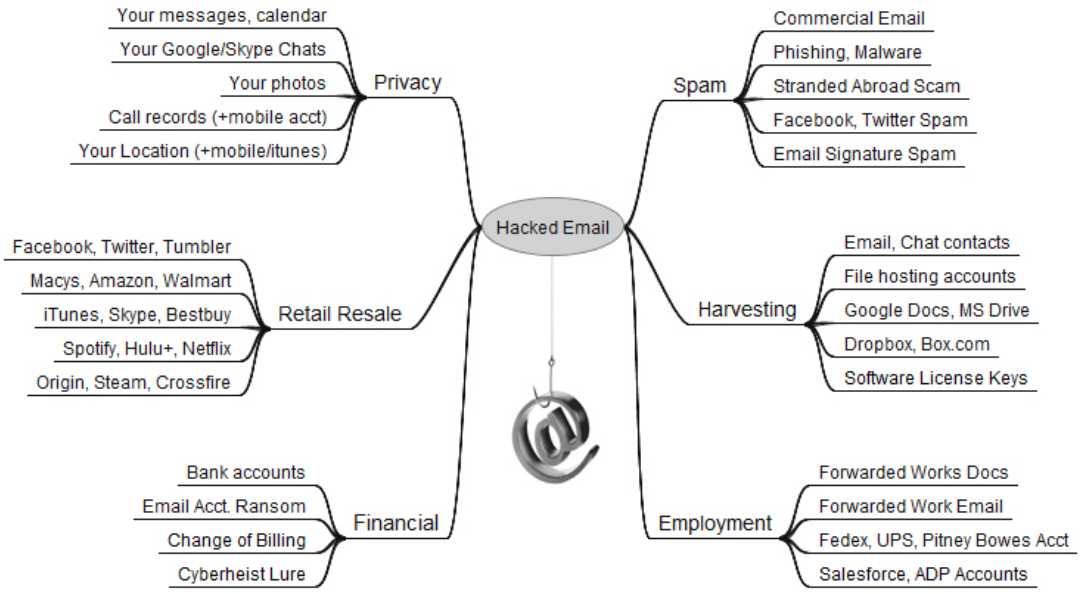
WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

stolen from the point of sale are known as "dumps."[8]

40. Once someone buys PII/PHI, it is then used to gain access to different areas of the victim's digital life, including bank accounts, social media, and credit card details. During that process, other sensitive data may be harvested from the victim's accounts, as well as from those belonging to family, friends, and colleagues.

41. In addition to PII/PHI, a hacked email account can be very valuable to cyber criminals. Since most online accounts require an email address not only as a username, but also as a way to verify accounts and reset passwords, a hacked email account could open up a number of other accounts to an attacker.[9]

42. As shown below, a hacked email account can be used to link to many other sources of information for an identity thief, including any purchase or account information found in the hacked email account.[10]



[8] *See All About Fraud: How Crooks Get the CVV*, Krebs on Security (April 26, 2016), https://krebsonsecurity.com/2016/04/all-about-fraud-how-crooks-get-the-cvv/ (last accessed February 8, 2023).

[9] *Identity Theft and the Value of Your Personal Data*, Trend Micro (Apr. 30, 2015), https://www.trendmicro.com/vinfo/us/security/news/online-privacy/identity-theft-and-the-value-of-your-personal-data. (last accessed February 8, 2023.)

[10] Brian Krebs, *The Value of a Hacked Email Account*, Krebs on Security (June 13, 2013), https://krebsonsecurity.com/2013/06/the-value-of-a-hacked-email-account/. (last accessed February 8, 2023).

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

43. Hacked information can also enable thieves to obtain other personal information through "phishing." According to the Report on Phishing available on the United States, Department of Justice's website: "AT&T, a large telecommunications company, had its sales system hacked into, resulting in stolen order information including full names and home addresses, order numbers and credit card numbers. The hackers then sent each customer a highly personalized e-mail indicating that there had been a problem processing their order and re-directing them to a spoofed website where they were prompted to enter further information, including birthdates and Social Security numbers."[11]

H. The Data Breach Has and Will Result in Additional Identity Theft and Identity Fraud

44. Defendant failed to implement and maintain reasonable security procedures and practices appropriate to protect the PII/PHI of Plaintiff and the Class Members. The ramification of Defendant's failure to keep Plaintiff and the Class Members' data secure is severe.

45. Between 2005 and 2019, at least 249 million individuals were affected by health care data breaches.[12] In 2019 alone, over 505 data HIPAA data breaches were reported, resulting in over 41 million healthcare records being exposed, stolen, or unlawfully disclosed.[13] The frequency and severity of healthcare data breaches has only increased with time. 2021 was reported as the "worst ever year" for healthcare data breaches—with at least 44,993,618 healthcare records having been exposed or stolen across 585 breaches.[14]

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

[11] *Report on Phishing* (Oct. 2006), https://www.justice.gov/archive/opa/docs/report_on_phishing.pdf (last accessed February 8, 2023).

[12] *Healthcare Data Breaches: Insights and Implications*, National Library of Medicine (May 13, 2020), https://www.ncbi.nlm.nih.gov/ pmc/articles/PMC7349636/. (last accessed February 8, 2023).

[13] *December 2019 Healthcare Data Breach*, HIPAA Journal (Jan 21, 2020), https://www.hipaajournal.com/december-2019-healthcare-data-breach-report/ (last accessed February 8, 2023).

[14] "Largest Healthcare Data Breaches of 2021," HIPPA Journal (Dec. 30, 2021), https://www.hipaajournal.com/largest-healthcare-data-breaches-of-2021/ (last accessed February 8, 2023).

46. It is incorrect to assume that reimbursing a consumer for a financial loss due to fraud makes that individual whole again. On the contrary, after conducting a study, the Department of Justice's Bureau of Justice Statistics ("BJS") found that "among victims who had personal information used for fraudulent purposes, about a third (32%) spent a month or more resolving problems."[15] In fact, the BJS reported, "resolving the problems caused by identity theft [could] take more than a year for some victims." *Id*.

I. Annual Monetary Losses from Identity Theft are in the Billions of Dollars

47. Javelin Strategy and Research reports that losses from identity theft reached $21 billion in 2013. There may be a time lag between when harm occurs and when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), 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 to Congressional Requesters (June 2007), http://www.gao.gov/new.items/d07737.pdf. (last accessed February 8, 2022.)

48. This is particularly the case with HIPAA data breaches such as Defendant's, as the information implicated, such as social security numbers of medical history, cannot be changed. Once such information is breached, malicious actors can continue misusing the stolen information for years to come. Indeed, medical identity theft are one of the most common, most expensive, and most difficult-to-prevent forms of identity theft.[16] Victims of medical identity theft "often

[15] *See Victims of Identity Theft*, U.S. Department of Justice (September 2015, revised November 13, 2017), https://bjs.ojp.gov/content/pub/pdf/vit14.pdf (last accessed February 8, 2023).

[16] Michael Ollove, *The Rise of Medical Identity Theft in Healthcare* (Feb. 7, 2014), https://khn.org/news/rise-of-indentity-theft/. (last accessed February 8, 2023).

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

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."[17]

49. Indeed, a study by Experian found that the average total cost of medical identity theft is "nearly $13,500" per incident, and that many victims were forced to pay out-of-pocket costs for fraudulent medical care.[18] Victims of healthcare data breaches often find themselves "being denied care, coverage or reimbursement by their medical insurers, having their policies canceled or having to pay to reinstate their insurance, along with suffering damage to their credit ratings and scores."[19]

50. Plaintiff and the Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any financial or identity fraud they suffer.

J. Plaintiff and Class Members Suffered Damages

51. The exposure of Plaintiff and Class Members' PII/PHI to unauthorized third-party hackers was a direct and proximate result of Defendant's failure to properly safeguard and protect Plaintiff and Class Members' PII from unauthorized access, use, and disclosure, as required by and state and federal law. Upon information and belief, the data breach was also a result of Defendant's failure to establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiff and Class Members' PII in order to protect against reasonably foreseeable threats to the security or integrity of such information, also required by their contracts and federal statute and regulation.

52. Plaintiff and Class Members' PII/PHI is private and sensitive in nature and was inadequately protected by Defendant. Defendant did not obtain Plaintiff and Class Members' consent to disclose their PII, except to certain persons not relevant to this action, as required by applicable law and industry standards.

---

[17] *Id.*

[18] *Healthcare Data Breach: What to Know About them and What to Do After One*, EXPERIAN (June 14, 2018), https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/. (last accessed February 8, 2023).

[19] *Id.*

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

53. As a direct and proximate result of Defendant's wrongful actions and inaction and the resulting data breach, Plaintiff and Class Members have been placed at an imminent, immediate, and continuing risk of harm from identity theft and identity fraud, requiring them to take the time and effort to mitigate the actual and potential impact of the subject data breach on their lives by, among other things, paying for credit and identity monitoring services, spending time on credit and identity monitoring, placing "freezes" and "alerts" with credit reporting agencies, contacting their personal, financial and healthcare institutions, closing or modifying personal, financial or healthcare accounts, and closely reviewing and monitoring their credit reports, financial accounts and healthcare accounts for unauthorized activity.

54. Plaintiff and Class Members also lost the value of their PII/PHI. PII/PHI is a valuable commodity, as evidenced by numerous companies which purchase PII from consumers, such as UBDI, which allows its users to link applications like Spotify, Twitter, or Apple Health and opt-in to paid opportunities to earn income, and Brave, which uses a similar business model, and by market-based pricing data involving the sale of stolen PII across multiple different illicit websites.

55. Top10VPN, a secure network provider, has compiled pricing information for stolen PII, including $160.15 for online banking details, $35.00 for credit reports, and $62.61 for passports. Standalone Yahoo email accounts have been listed for as little as $0.41, while banking logins are in the range of $500, and verified Paypal accounts with high balances are listed at as much as $2,000.

56. In addition, Privacy Affairs, a cyber security research firm, has listed the following prices for stolen PII:

U.S. driving license, high quality:	$550
Auto insurance card:	$70
AAA emergency road service membership card:	$70
Wells Fargo bank statement:	$25
Wells Fargo bank statement with transactions:	$80
Rutgers State University student ID:	$70

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

57. Finally, Plaintiff and Class Members have lost the benefit of their bargains. Plaintiff and Class members entered into agreements with Defendant under the reasonable but mistaken belief that it would reasonably and adequately protect their PII/PHI and would not have entered into such agreements had they known that Defendant would not reasonably and adequately protect their PII/PHI. Plaintiff and Class Members have thus suffered actual damages in an amount at least equal to the difference in value between the medical services that include reasonable and adequate data security that they bargained for, and the medical services that do not that they actually received.

58. Defendant's wrongful actions and inaction directly and proximately caused the theft and dissemination into the public domain of Plaintiff and Class Members' PII/PHI, causing them to suffer, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including:

a. The improper disclosure and theft of their PII/PHI;

b. The imminent and impending injury flowing from potential fraud and identity theft posed by their PII/PHI being exposed to and misused by unauthorized third-party hackers;

c. The untimely and inadequate notification of the data breach;

d. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the data breach; and

e. Ascertainable losses in the form of deprivation of the value of their PII/PHI, for which there is a well-established national and international market.

CLASS ACTION ALLEGATIONS

59. Plaintiff brings this action on behalf of himself and on behalf of all other persons similarly situated pursuant to Rules 23(b)(2), (b)(3) and (c)(4) of the Federal Rules of Civil Procedure.

///

///

///

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

60. Plaintiff seeks to certify following Classes, as defined below:

All persons residing in the United States whose PII and PHI was compromised by the data breach disclosed by Defendant Community Psychiatry Management, LLC dba Mindpath Health on or about January 9, 2023.

61. Excluded from the Classes is Defendant, including any entity in which Defendant has a controlling interest, is a parent or subsidiary, or which is controlled by Defendant, as well as the officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns of Defendant. Also excluded are the judge and the court personnel in this case and any members of their immediate families. Plaintiff reserves the right to amend the Class definition if discovery and further investigation reveal that the Class should be expanded or otherwise modified.

62. *Numerosity*. The Members of the Classes are so numerous that joinder of all of them is impracticable. At this present moment, the Class is comprised of at least 193,947 individuals. The disposition of the claims of Class Members in a single action will provide substantial benefits to all parties and to the Court. The Class Members are readily identifiable from information and records in Defendant's possession, custody, or control, such as reservation receipts and confirmations.

63. *Commonality*. Fed. R. Civ. P. 23(a)(2) and (b)(3): 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 took reasonable steps and measures to safeguard Plaintiff' and Class Members' PII and PHI;

b. Whether Defendant violated common and statutory regulations and requirements by failing to implement reasonable procedures and practices;

c. Which security procedures and which data-breach notification procedure should Defendant be required to implement as part of any injunctive relief ordered by the Court;

d. Whether Defendant knew or should have known about the data breach prior to the disclosure;

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

e. Whether Defendant's acts or omissions described herein give rise to a claim of negligence;

f. Whether Defendant had a duty to promptly notify Plaintiff and Class Members that their PII was, or potentially could be, compromised;

g. What security measures, if any, must be implemented by Defendant to comply with its duties under state and federal law;

h. The nature of the relief, including equitable relief, to which Plaintiff and the Class Members are entitled; and

i. Whether Plaintiff and Class members are entitled to damages, civil penalties, and/or injunctive relief.

64. *Typicality*. Fed. R. Civ. P. 23(a)(3): Plaintiff' claims are typical of those of other Class Members because Plaintiff' PHI/PII, like that of every other Class Member, was collected by Defendant during its ordinary course of business and then subsequently misused and/or disclosed by Defendant.

65. *Adequacy of Representation*. Fed. R. Civ. P. 23(a)(4): Plaintiff' will fairly and adequately represent and protect the interests of the members of the Classes. Plaintiff have retained competent counsel experienced in litigation of class actions, including consumer and data breach class actions, and Plaintiff intend to prosecute this action vigorously. Plaintiff' claims are typical of the claims of other members of the Classes and Plaintiff have the same non-conflicting interests as the other Class Members. Therefore, the interests of the Classes will be fairly and adequately represented by Plaintiff and their counsel.

66. *Superiority of Class Action*. Fed. R. Civ. P. 23(b)(3): A class action is superior to other available methods for the fair and efficient adjudication of this controversy since joinder of all the members of the Class is impracticable. Furthermore, the adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially conflicting adjudication of the asserted claims. There will be no difficulty in the management of this action as a class action.

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

67. *Superiority of Class Action*. Fed. R. Civ. P. 23(b)(3): A class action is superior to other available methods for the fair and efficient adjudication of this controversy since joinder of all the members of the Class is impracticable. Furthermore, the adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially conflicting adjudication of the asserted claims. There will be no difficulty in the management of this action as a class action. Defendant has acted on grounds that apply generally to the Classes as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

68. Damages for any individual class member are likely insufficient to justify the cost of individual litigation so that, in the absence of class treatment, Defendant's violations of law inflicting substantial damages in the aggregate would go un-remedied.

69. Class certification is also appropriate under Fed. R. Civ. P. 23(a) and (b)(2), because Defendant has acted or refused to act on grounds generally applicable to the Classes, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Classes as a whole.

CAUSES OF ACTION

FIRST CAUSE OF ACTION

Negligence

70. Plaintiff repeats and incorporates herein by reference each and every allegation contained in paragraphs 1 through 69, inclusive, of this Complaint as if set forth fully herein.

71. Defendant requires any individual that uses its services to provide their PII and PHI to Defendant. Defendant collects and stores this PII and PHI as a part of its regular business activities, and for its own pecuniary gain.

72. Defendant owed Plaintiff and the Class Members a duty of care in the handling of its patient's PII. This duty included, but was not limited to, keeping that PII secure and preventing disclosure of the PII to any unauthorized third parties. This duty of care existed independently of Defendants' contractual duties to Plaintiff and the Class Members. Under the FTC Guidelines, and other sources of industry-wide cybersecurity standards, Defendant is obligated to incorporate

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

adequate measures to safeguard and protect PII that is entrusted to them in their ordinary course of business and transactions with customers.

73. Pursuant to the Federal Trade Commission Act (15 U. S. C. §45), Defendants had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff and Class Members' PII. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer information, treating the businesses' 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, 15 U.S.C. § 45. Orders from these actions further clarify the measures businesses are required to undertake in order to satisfy their data security obligations. [20]

74. Additional industry guidelines which provide a standard of care can be found in NIST's *Framework for Improving Critical Infrastructure Cybersecurity*.[21] NIST's Framework identifies seven steps for establishing or improving a cybersecurity program (section 3. 2). Those steps are:

> Step 1: Prioritize and Scope. The organization identifies its business/mission objectives and high-level organizational priorities. With this information, the organization makes strategic decisions regarding cybersecurity implementations and determines the scope of systems and assets that support the selected business line or process. The Framework can be adapted to support the different business lines or processes within an organization, which may have different business needs and associated risk tolerance. Risk tolerances may be reflected in a target Implementation Tier.

[20] Federal Trade Commission, *Privacy and Security Enforcement: Press Releases*, https://www.ftc.gov/news-events/topics/protecting-consumer-privacy-security/privacy-security-enforcement (last accessed February 8, 2023).

[21] "Framework for Improving Critical Infrastructure Cybersecurity," National Institute for Standards and Technology, https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf (last accessed February 8, 2023).

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

Step 2: Orient. Once the scope of the cybersecurity program has been determined for the business line or process, the organization identifies related systems and assets, regulatory requirements, and overall risk approach. The organization then consults sources to identify threats and vulnerabilities applicable to those systems and assets.

Step 3: Create a Current Profile. The organization develops a Current Profile by indicating which Category and Subcategory outcomes from the Framework Core are currently being achieved. If an outcome is partially achieved, noting this fact will help support subsequent steps by providing baseline information.

Step 4: Conduct a Risk Assessment. This assessment could be guided by the organization's overall risk management process or previous risk assessment activities. The organization analyzes the operational environment in order to discern the likelihood of a cybersecurity event and the impact that the event could have on the organization. It is important that organizations identify emerging risks and use cyber threat information from internal and external sources to gain a better understanding of the likelihood and impact of cybersecurity events.

Step 5: Create a Target Profile. The organization creates a Target Profile that focuses on the assessment of the Framework Categories and Subcategories describing the organization's desired cybersecurity outcomes. Organizations also may develop their own additional Categories and Subcategories to account for unique organizational risks. The organization may also consider influences and requirements of external stakeholders such as sector entities, customers, and business partners when creating a Target Profile. The Target Profile should appropriately reflect criteria within the target Implementation Tier.

Step 6: Determine, Analyze, and Prioritize Gaps. The organization compares the Current Profile and the Target Profile to determine gaps. Next, it

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

> creates a prioritized action plan to address gaps – reflecting mission drivers, costs and benefits, and risks – to achieve the outcomes in the Target Profile. The organization then determines resources, including funding and workforce, necessary to address the gaps. Using Profiles in this manner encourages the organization to make informed decisions about cybersecurity activities, supports risk management, and enables the organization to perform cost-effective, targeted improvements.
>
> Step 7: Implement Action Plan. The organization determines which actions to take to address the gaps, if any, identified in the previous step and then adjusts its current cybersecurity practices in order to achieve the Target Profile. For further guidance, the Framework identifies example Informative References regarding the Categories and Subcategories, but organizations should determine which standards, guidelines, and practices, including those that are sector specific, work best for their needs.

75. In addition to their obligations under federal regulations and industry standards, Defendant owed a duty to Plaintiff and the Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII/PHI in their possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendant owed a duty to Plaintiff and the Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that their computer systems and networks, and the personnel responsible for them, adequately protected the PII/PHI of Plaintiff and the Class Members.

76. Defendant owed a duty to Plaintiff and the Class Members to design, maintain, and test their internal data systems to ensure that the PII/PHI in Defendant's possession was adequately secured and protected.

77. Defendant owed a duty to Plaintiff and the Class Members to create and implement reasonable data security practices and procedures to protect the PII/PHI in its custodianship,

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

including adequately training its employees and others who accessed PII/PHI within its computer systems on how to adequately protect PII/PHI.

78. Defendant owed a duty to Plaintiff and the Class Members to implement processes or safeguards that would detect a breach of their data security systems in a timely manner.

79. Defendant owed a duty to Plaintiff and the Class Members to act upon data security warnings and alerts in a timely fashion.

80. Defendant owed a duty to Plaintiff and the Class Members to timely disclose if its computer systems and data security practices were inadequate to safeguard individuals' PII from theft because such an inadequacy would be a material consideration in Plaintiff and Class Members' decisions to entrust their PHI/PII to Defendants.

81. Defendant owed a duty to Plaintiff and the Class Members to disclose in a timely and accurate manner when data breaches occur.

82. Defendant owed a duty of care to Plaintiff and the Class Members because they were foreseeable and probable victims of any inadequate data security practices and systems. Defendant collected PII from Plaintiff and the Class Members. Defendants knew that a breach of its data systems would cause Plaintiff and the Class Members to incur damages.

83. Defendants breached its duties of care to safeguard and protect the PII/PHI which Plaintiff and the Class Members entrusted to it. Upon information and belief, Defendant adopted inadequate safeguards to protect the PII/PHI and failed to adopt industry-wide standards set forth above in its supposed protection of the PII/PHI. Defendant failed to design, maintain, and test its computer system to ensure that the PII/PHI was adequately secured and protected, failed to create and implement reasonable data security practices and procedures, failed to implement processes that would detect a breach of its data security systems in a timely manner, failed to disclose the breach to potentially affected customers in a timely and comprehensive manner, and otherwise breached each of the above duties of care by implementing careless security procedures which led directly to the breach.

84. Defendant breached the duties set forth in 15 U.S.C. §45, the FTC guidelines, the NIST's Framework for Improving Critical Infrastructure Cybersecurity, and other industry

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

guidelines. In violation of 15 U.S.C. §45, Defendant failed to implement proper data security procedures to adequately and reasonably protect Plaintiff and Class Member's PII/PHI. In violation of the FTC guidelines, *inter alia*, Defendant did not protect the personal customer information that it keeps; failed to properly dispose of personal information that was no longer needed; failed to encrypt information stored on computer networks; lacked the requisite understanding of their network's vulnerabilities; and failed to implement policies to correct security problems. In violation of the NIST's Framework, Defendant, *inter alia*, failed to adopt sufficient resources to identity and address security gaps.

85. Defendant's failure to comply with applicable laws and regulations constitutes negligence per se.

86. As a direct and proximate result of Defendant's failure to adequately protect and safeguard the PII, Plaintiff and the Class members suffered damages. Plaintiff and the Class Members were damaged because their PII was accessed by third parties, resulting in increased risk of identity theft, property theft and extortion for which Plaintiff and the Class Members were forced to adopt preventive and remedial efforts. These damages were magnified by the passage of time because Defendant failed to notify Plaintiff and Class Members of the data breach until weeks had passed. In addition, Plaintiff and Class Members were also damaged in that they must now spend copious amounts of time combing through their records in order to ensure that they do not become the victims of fraud and/or identity theft.

87. Plaintiff and Class Members have suffered actual injury and are entitled to damages in an amount to be proven at trial but in excess of the minimum jurisdictional requirement of this Court.

SECOND CAUSE OF ACTION

Breach of Implied Contract

88. Plaintiff repeats and incorporates herein by reference each and every allegation contained in paragraphs 1 through 87, inclusive, of this Complaint as if set forth fully herein.

89. Plaintiff and Class Members entered into agreements for medical treatment with Defendant. In making those agreements, Defendant solicited and invited Plaintiff and Class

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

Members to provide their PII and PHI to Defendant as requirement of receiving service. Plaintiff and Class and Members accepted Defendant's offers and provided their PII and PHI to enter the agreements. Inherent within those agreements was an implied contractual obligation that Defendant would implement reasonable and adequate data security to safeguard and protect the PII and PHI entrusted to them by Plaintiff and Class Members from unauthorized disclosure.

90. Thus, when Plaintiff and Class Members provided their PII and PHI to Defendant in exchange for medical services, they entered into implied contracts with Defendant under which Defendant agreed to and was obligated to reasonably protect their PII and PHI. Plaintiff and Class provided payment to Defendant, as well as their PII and PHI, under the reasonable but mistaken belief that any money they paid to Defendant in connection to its provision of medical services would be used in part to provide reasonable and adequate data security for their PII and PHI.

91. This implied contract is acknowledged and memorialized in Defendant's customer-facing documents, including, *inter alia*, Defendant's HIPAA Notice of Privacy Practices, wherein it states that "[w]e understand the importance of privacy and are committed to maintaining the confidentiality of your medical information," and "[e]xcept as described in this Notice of Privacy Practices, this medical practice will not use or disclose PHI without your written authorization."

92. Defendant did not provide reasonable and adequate data security for Plaintiff and Class Member's PII and PHI, and instead caused it to be disclosed to unauthorized third-party hackers. Defendant did not comply with federal statute and regulation and did not comply with industry data security standards. In doing so, Defendant materially breached their obligations under implied contract.

93. That Defendant would implement such reasonable and adequate data security was a material prerequisite to the agreements between Plaintiff and Class Members. Reasonable consumers value the privacy of their PII and PHI, and do not enter into agreements for medical services with healthcare providers which are known not to protect customer data. Accordingly, Plaintiff and Class Members would not have entered into agreements with Defendant and would not have provided them with their sensitive PII and PHI, had they known that Defendant would not implement such reasonable and adequate data security.

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

94. As a result of Defendant's breach, Plaintiff and Class Members have lost the benefit of their bargains. Plaintiff and Class members entered into agreements with Defendant under the reasonable but mistaken belief that it would reasonably and adequately protect their PII/PHI and would not have entered into such agreements had they known that Defendant would not reasonably and adequately protect their PII/PHI. Plaintiff and Class Members have thus suffered actual damages in an amount at least equal to the difference in value between the medical services that include reasonable and adequate data security that they bargained for, and the medical services that do not that they actually received.

95. Plaintiff and Class Members fully performed their obligations under the implied contract by providing their PII/PHI and making payments to Defendant.

96. Plaintiff and Class Members have suffered actual injury and are entitled to damages in an amount to be proven at trial but in excess of the minimum jurisdictional requirement of this Court.

THIRD CAUSE OF ACTION

Breach of Fiduciary Duty

97. Plaintiff repeats and incorporates herein by reference each and every allegation contained in paragraphs 1 through 96, inclusive, of this Complaint as if set forth fully herein.

98. Plaintiff and Class Members provided their PII and PHI to Defendant in confidence and under the reasonable but mistaken belief that Defendant would protect the confidentiality of that information. Plaintiff and Class Members would not have provided Defendant with their PII and PHI had they known that Defendant would not take reasonable and adequate steps to protect it.

99. Defendant's acceptance and storage of Plaintiff; and Class Members' PII and PHI created a fiduciary relationship between Defendant and Plaintiff and Class Members. As a fiduciary of Plaintiff and Class Members, Defendant has duty to act primarily for the benefit of its patients and health plan participants, which includes implementing reasonable, adequate, and statutorily complaint safeguards to protect Plaintiff' and Class Members' PII and PHI.

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

100. Defendant breached its fiduciary duties to Plaintiff and Class Members by, *inter alia,* failing to implement reasonable and adequate data security protections, failing to comply with the data security guidelines set forth by the FTC, NIST and HIPAA, failing to implement reasonable and adequate data security training for its employees, and otherwise failing to reasonably and adequately safeguard the PII and PHI of Plaintiff and Class Members.

101. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and Class Members have suffered damages. Plaintiff and the Class Members were damaged because their PII was accessed by third parties, resulting in increased risk of identity theft, property theft and extortion for which Plaintiff and the Class Members were forced to adopt preventive and remedial efforts. These damages were magnified by the passage of time because Defendant failed to notify Plaintiff and Class Members of the data breach until weeks had passed. In addition, Plaintiff and Class Members were also damaged in that they must now spend copious amounts of time combing through their records in order to ensure that they do not become the victims of fraud and/or identity theft.

102. Plaintiff and Class Members have suffered actual injury and are entitled to damages in an amount to be proven at trial but in excess of the minimum jurisdictional requirement of this Court.

FOURTH CAUSE OF ACTION

Unjust Enrichment

103. Plaintiff repeats and incorporates herein by reference each and every allegation contained in paragraphs 1 through 102, inclusive, of this Complaint as if set forth fully herein.

104. Plaintiff and Class Members provided their PII and PHI and conferred a monetary benefit upon Defendant in exchange for healthcare services. Plaintiff and Class Members did so under the reasonable but mistaken belief that part of their monetary payment to Defendant would cover the implementation of reasonable, adequate, and statutorily mandated safeguards to protect their PII and PHI. Defendant was enriched when it sold its healthcare services at a higher price than it otherwise would have based on those reasonable but mistaken beliefs.

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

105. Defendant's enrichment came at the expense of Plaintiff and Class Members, who would not have paid for Defendant's services, or would have only been willing to paid substantially less for them, had they been aware that Defendant had not implement reasonable, adequate and statutorily mandated safeguards to protect their PII and PHI.

106. As a direct and proximate result of Defendant's wrongful actions and inactions, Plaintiff and Class Members suffered have suffered damages in the form of their lost benefit of the bargains. Plaintiff and Class members entered into agreements with Defendant under the reasonable but mistaken belief that it would reasonably and adequately protect their PII/PHI and would not have entered into such agreements had they known that Defendant would not reasonably and adequately protect their PII/PHI. Plaintiff and Class Members have thus suffered actual damages in an amount at least equal to the difference in value between the medical services that include reasonable and adequate data security that they bargained for, and the medical services that do not that they actually received.

107. Defendant should not be permitted to retain Plaintiff' and Class Members' lost benefits, without having adequately implemented the data privacy and security procedures for itself that Plaintiff and Class Members paid for and that were otherwise mandated by federal, state, and local laws. and industry standards. Defendant should not be allowed to benefit at the expense of consumers who trust Defendant to protect the PII and PHI that they are required to provide to Defendant in order to receive Defendant's services.

108. As a direct and proximate result of Defendants' fraudulent conduct, Plaintiff and Class members have suffered injury and are entitled to damages in an amount to be proven at trial but in excess of the minimum jurisdictional requirement of this Court.

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all of the Class Members, respectfully requests that the Court enter judgment in his favor and against Defendant as follows:

a. For an Order certifying the Class as defined herein and appointing Plaintiff and their 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' and Class Members' PII/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 to Class Members the type of PII compromised.

d. For an award of actual damages, statutory damages, and compensatory damages, in an amount to be determined at trial;

e. For an award of punitive and treble damages, in an amount to be determined at trial;

f. For an award of costs of suit, litigation expenses and attorneys' fees, as allowable by law; and

g. For such other and further relief as this Court may deem just and proper.

h. Pre and post-judgment interest on any amounts awarded; and

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

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

DEMAND FOR JURY TRIAL

Plaintiff, on behalf of himself and all others similarly situated, hereby demands a jury trial for all claims so triable.

Dated: February 9, 2023

Respectfully Submitted by:

WILSHIRE LAW FIRM, PLC

/s/ Thiago M. Coelho

Thiago M. Coelho
3055 Wilshire Blvd., FL 12
Los Angeles, CA 90010
Tel: (213) 381-9988
Fax: (213) 381-9989
thiago@wilshirelawfirm.com

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

ClassAction.org