Daniel Srourian, Esq. [SBN 285678]
SROURIAN LAW FIRM, P.C.
3435 Wilshire Blvd., Suite 1710
Los Angeles, CA 90010
Telephone: (213) 474-3800
Fax: (213) 471-4160
Email: daniel@slfla.com

Attorneys for Representative Plaintiff

IN THE SUPERIOR COURT OF THE STATE OF CALIFORNIA

IN AND FOR THE COUNTY OF TULARE

DAVID UNDERWOOD, individually, and on behalf of all others similarly situated,

Plaintiff,

vs.

HAPY BEAR SURGERY CENTER, LLC; and DOES 1 through 100, inclusive,

Defendants.

Case No. VCU307987

CLASS ACTION

COMPLAINT FOR DAMAGES, INJUNCTIVE AND EQUITABLE RELIEF FOR:

1. **NEGLIGENCE;**
2. **BREACH OF IMPLIED CONTRACT;**
3. **VIOLATION OF THE CONFIDENTIALITY OF MEDICAL INFORMATION ACT (CAL. CIV. CODE §56);**
4. **VIOLATION OF CAL. BUS. & PROF. CODE §17200;**
5. **UNJUST ENRICHMENT**

[JURY TRIAL DEMANDED]

Representative Plaintiff alleges as follows:

INTRODUCTION

1. Representative Plaintiff Davud Underwood ("Representative Plaintiff(s)"), brings this class action against Defendant Hapy Bear Surgery Center, LLC, and Does 1-100 (collectively "Defendants") for their failure to properly secure and safeguard Class Members' protected health information and personally identifiable information stored within Defendants' network and

systems, including, without limitation, full name, address, medical information, health insurance information, social security number, and driver's license number (these types of information, *inter alia*, being thereafter referred to, collectively, as "protected health information" or "PHI"[1] and "personally identifiable information" or "PII").[2]

2. With this action, Representative Plaintiff(s) seek to hold Defendants responsible for the harms it caused and will continue to cause Representative Plaintiff(s) and others similarly situated persons in the massive and preventable cyberattack purportedly discovered by Defendants on s, by which unauthorized actors infiltrated Defendants' inadequately protected systems and accessed highly sensitive PHI/PII, which was being kept unprotected (the "Data Breach").

3. Representative Plaintiff(s) further seek to hold Defendants responsible for not ensuring that the PHI/PII was maintained in a manner consistent with industry, the Health Insurance Portability and Accountability Act of 1996 ("HIPPA") Privacy Rule (45 CFR, Part 160 and Parts A and E of Part 164), the HIPPA Security Rule (45 CFR Part 160 and Subparts A and C of Part 164), and other relevant standards.

4. While Defendants experienced a "network disruption" as early as December 27, 2023, Defendants did not begin informing victims of the Data Breach until April 11, 2024, and failed to inform victims when or for how long the Data Breach occurred. Indeed, Representative Plaintiff(s) and Class Members were wholly unaware of the Data Breach until they received letters from Defendants informing them of it. The notice received by Representative Plaintiff(s) was dated April 11, 2024. *See Exhibit A.*

---

[1] Personal health information ("PHI") is a category of information that refers to an individual's medical records and history, which is protected under the Health Insurance Portability and Accountability Act. *Inter alia*, PHI includes test results, procedure descriptions, diagnoses, personal or family medical histories and data points applied to a set of demographic information for a particular patient.

[2] Personally identifiable information ("PII") generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual. PHI/PII also is generally defined to include certain identifiers that do not on its face name an individual, but that are considered to be particularly sensitive and/or valuable if in the wrong hands (for example, Social Security numbers, passport numbers, driver's license numbers, financial account numbers).

5. Defendants acquired, collected and stored Representative Plaintiff(s)' and Class Members' PHI/PII and/or financial information. Therefore, at all relevant times, Defendants knew, or should have known, that Representative Plaintiff(s) and Class Members would use Defendants' services to store and/or share sensitive data, including highly confidential PHI/PII.

6. HIPAA establishes national minimum standards for the protection of individuals' medical records and other personal health information. HIPAA, generally, applies to health plans/insurers, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically, and sets minimum standards for Defendants' maintenance of Representative Plaintiff(s)' and Class Members' PHI/PII. More specifically, HIPAA requires appropriate safeguards be maintained by organizations such as Defendants to protect the privacy of personal health information and sets limits and conditions on the uses and disclosures that may be made of such information without customer/patient authorization. HIPAA also establishes a series of rights over Representative Plaintiff(s)' and Class Members' PHI/PII, including rights to examine and obtain copies of their health records, and to request corrections thereto.

7. Additionally, the HIPAA Security Rule establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity. The HIPAA Security Rule requires appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information.

8. By obtaining, collecting, using, and deriving a benefit from Representative Plaintiff(s)' and Class Members' PHI/PII, Defendants assumed legal and equitable duties to those individuals. These duties arise from HIPAA and other state and federal statutes and regulations as well as common law principles. Representative Plaintiff(s) do/does not bring claims in this action for direct violations of HIPAA, but charge(s) Defendants with various legal violations merely predicated upon the duties set forth in HIPAA.

9. Defendants disregarded the rights of Representative Plaintiff(s) and Class Members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that Representative Plaintiff(s)' and Class Members' PHI/PII was

safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As a result, the PHI/PII of Representative Plaintiff(s) and Class Members was compromised through disclosure to an unknown and unauthorized third party—an undoubtedly nefarious third party that seeks to profit off this disclosure by defrauding Representative Plaintiff(s) and Class Members in the future. Representative Plaintiff(s) and Class Members have a continuing interest in ensuring that their information is and remains safe, and they are entitled to injunctive and other equitable relief.

JURISDICTION AND VENUE

10. This Court has jurisdiction over Representative Plaintiff's and Class Members' claims for damages and injunctive relief pursuant to, *inter alia*, Cal. Civ. Code §56, *et seq*. (Confidentiality of Medical Information Act), and Cal. Bus. & Prof. Code §17200, *et seq.*, among other California state statues.

11. Venue as to Defendants is proper in this judicial district pursuant to California Code of Civil Procedure § 395(a). Defendants are a California Limited Liability Corporation based out of Tulare, California. The unlawful acts alleged herein have had a direct effect on Representative Plaintiff and those similarly situated within the State of California and within this County.

PLAINTIFF(S)

12. Representative Plaintiff is an adult individual and, at all relevant times herein, a resident and citizen of the State of California. Representative Plaintiff is a victim of the Data Breach.

13. Defendants received highly sensitive personal, health, and insurance information from Representative Plaintiff and Class Members in connection with medical services they received or requested from Defendants. As a result, Representative Plaintiff(s)' and Class Members' information was among the data accessed by an unauthorized third-party in the Data Breach.

14. Representative Plaintiff(s) received—and were "consumers" for purposes of obtaining services from Defendants within this state.

15. At all times herein relevant, Representative Plaintiff(s) are and were members of each of the Classes.

16. Representative Plaintiff(s)' PHI/PII was exposed in the Data Breach because Defendants stored and/or shared Representative Plaintiff(s)' PHI/PII. Representative Plaintiff(s)' PHI/PII was within the possession and control of Defendants at the time of the Data Breach.

17. Representative Plaintiff(s) suffered actual injury in the form of damages to and diminution in the value of their PHI/PII—a form of intangible property that they entrusted to Defendant, which was compromised in and as a result of the Data Breach.

18. Representative Plaintiff(s) and Class Members suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of privacy, as well as anxiety over the impact of cybercriminals accessing, using, and selling his/her/their PHI/PII and/or financial information.

19. Representative Plaintiff(s) and Class Members have suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from their PHI/PII, in combination with their name, being placed in the hands of unauthorized third-parties/criminals.

20. Representative Plaintiff(s) and Class Members have a continuing interest in ensuring that their PHI/PII, which, upon information and belief, remains backed up in Defendants' possession, is protected and safeguarded from future breaches.

21. Representative Plaintiff(s) is/are unaware of the true names and capacities of those defendants sued herein as Does 1 through 100, inclusive and, therefore, sue(s) these defendants by such fictitious names. The Representative Plaintiff(s) will seek leave of court to amend this Complaint when such names are ascertained. Representative Plaintiff is informed and believes and, on that basis, alleges that each of the fictitiously-named defendants were responsible in some manner for, gave consent to, ratified, and/or authorized the conduct herein alleged and that the damages, as herein alleged, were proximately caused thereby.

22. Representative Plaintiff is informed and believes and, on that basis, alleges that, at all relevant times herein mentioned, each of the defendants was the agent and/or employee of each

of the remaining defendants and, in doing the acts herein alleged, was acting within the course and scope of such agency and/or employment.

COMMON FACTUAL ALLEGATIONS

The Cyberattack

23. On December 27, 2023, Defendant Hapy Bear Surgery Center fell victim to a cyberattack that affected the functionality and availability of some of its IT systems.

24. These unauthorized individuals had access to users' personal information, including their full name, address, medical information, health insurance information, social security number, and driver's license number according to the letter.

Defendants' Failed Response to the Breach

25. Upon information and belief, the unauthorized third-parties gained access to Representative Plaintiff's and Class Members' PHI/PII with the intent of engaging in misuse of the PII, including marketing and selling Representative Plaintiff's and Class Members' PII.

26. Not until roughly two months after they claim to have discovered the Data Breach did Defendants begin sending notices to persons whose PHI/PII Defendants confirmed was potentially compromised as a result of the Data Breach ("The Notice"). The Notice provided basic details of the Data Breach and Defendant's recommended next steps.

27. The Notice included, *inter alia*, allegations that Defendants had experienced the Data Breach on December 27, 2023 and had taken steps to respond. But the Notice lacked sufficient information as to how the breach occurred and where the information hacked may be today.

28. Upon information and belief, the unauthorized third-parties gained access to Representative Plaintiff(s)' and Class Members' PHI/PII with the intent of engaging in misuse of the PHI/PII, including marketing and selling Representative Plaintiff(s)' and Class Members' PHI/PII.

29. Defendants have and continue to have obligations created by HIPAA, applicable federal and state law as set forth herein, reasonable industry standards, common law, and their own

assurances and representations to keep Representative Plaintiff(s)' and Class Members' PHI/PII confidential and to protect such PHI/PII from unauthorized access.

30. Representative Plaintiff(s) and Class Members were required to provide their PHI/PII to Defendants in order to receive benefits from Defendant and utilize the BenefitsCal portal. As part of providing their services, Defendants created, collected, and stored Representative Plaintiff(s) and Class Members with the reasonable expectation and mutual understanding that Defendants would comply with their obligations to keep such information confidential and secure from unauthorized access.

31. Despite this, Representative Plaintiff(s) and the Class Members remain, even today, in the dark regarding what particular data was confirmed stolen, and what steps are being taken, if any, to secure their PHI/PII going forward. Representative Plaintiff(s) and Class Members are, thus, left to speculate as to where their PHI/PII ended up, who has used it and for what potentially nefarious purposes. Indeed, they are left to further speculate as to the full impact of the Data Breach and how exactly Defendants intend to enhance their information security systems and monitoring capabilities so as to prevent further breaches.

32. Representative Plaintiff(s)' and Class Members' PHI/PII may end up for sale on the dark web, or simply fall into the hands of companies that will use the detailed PHI/PII for targeted marketing without the approval of Representative Plaintiff(s) and/or Class Members. either way, unauthorized individuals can now easily access the PHI/PII of Representative Plaintiff(s) and Class Members.

Defendants Collected/Stored Class Members' PHI/PII

33. Defendants acquired, collected, and stored and assured reasonable security over Representative Plaintiff(s)' and Class Members' PHI/PII.

34. As a condition of their relationships with Representative Plaintiff(s) and Class Members, Defendants required that Representative Plaintiff(s) and Class Members entrust Defendants with highly sensitive and confidential PHI/PII. Defendant, in turn, stored that information of Defendants' system that was ultimately affected by the Data Breach.

35. By obtaining, collecting, and storing Representative Plaintiff(s)' and Class Members' PHI/PII, Defendants assumed legal and equitable duties and knew or should have known that they were thereafter responsible for protecting Representative Plaintiff(s)' and Class Members' PHI/PII from unauthorized disclosure.

36. Representative Plaintiff(s) and Class Members have taken reasonable steps to maintain the confidentiality of their PHI/PII. Representative Plaintiff(s) and Class Members relied on Defendants to keep their PHI/PII confidential and securely maintained, to use this information for business and healthcare purposes only, and to make only authorized disclosures of this information.

37. Defendants could have prevented the Data Breach, which began as early as December 27, 2023 by properly securing and encrypting and/or more securely encrypting their servers generally, as well as Representative Plaintiff(s)' and Class Members' PHI/PII.

38. Defendants' negligence in safeguarding Representative Plaintiff(s)' and Class Members' PHI/PII is exacerbated by repeated warnings and alerts directed to protecting and securing sensitive data, as evidenced by the trending data breach attacks in recent years.

39. The healthcare industry has experienced a large number of high-profile cyberattacks even in just the short period preceding the filing of this Complaint and cyberattacks, generally, have become increasingly more common. More healthcare data breaches were reported in 2020 than in any other year, showing a 25% increase.[3] Additionally, according to the HIPAA Journal, the largest healthcare data breaches have been reported in April 2021.[4]

40. For example, Universal Health Services experienced a cyberattack on September 29, 2020 that appears similar to the attack on Defendant. As a result of this attack, Universal Health Services suffered a four-week outage of its systems which caused as much as $67 million in recovery costs and lost revenue.[5] Similarly, in 2021, Scripps Health suffered a cyberattack, an

[3] https://www.hipaajournal.com/2020-healthcare-data-breach-report-us/ (last accessed November 5, 2021).
[4] https://www.hipaajournal.com/april-2021-healthcare-data-breach-report/ (last accessed November 5, 2021).
[5] https://ir.uhsinc.com/news-releases/news-release-details/universal-health-services-inc-reports-2020-fourth-quarter-and (last accessed November 5, 2021).

event which effectively shut down critical health care services for a month and left numerous patients unable to speak to its physicians or access vital medical and prescription records.[6] A few months later, University of San Diego Health suffered a similar attack.[7]

41. Due to the high-profile nature of these breaches, and other breaches of its kind, Defendants was and/or certainly should have been on notice and aware of such attacks occurring in the healthcare industry and, therefore, should have assumed and adequately performed the duty of preparing for such an imminent attack. This is especially true given that Defendants are large, sophisticated operations with the resources to put adequate data security protocols in place.

42. Yet, despite the prevalence of public announcements of data breach and data security compromises, Defendants failed to take appropriate steps to protect Representative Plaintiff(s)' and Class Members' PHI/PII from being compromised.

Defendants Had an Obligation to Protect the Stolen Information

43. Defendants' failure to adequately secure Representative Plaintiff(s)' and Class Members' sensitive data breaches duties it owes Representative Plaintiff(s) and Class Members under statutory and common law. Under HIPAA, health insurance providers have an affirmative duty to keep patients' Protected Health Information private. As a covered entity, Defendants had a statutory duty under HIPAA and other federal and state statutes to safeguard Representative Plaintiff(s)' and Class Members' data. Moreover, Representative Plaintiff(s) and Class Members surrendered their highly sensitive personal data to Defendants under the implied condition that Defendants would keep it private and secure. Accordingly, Defendants also had an implied duty to safeguard their data, independent of any statute.

44. Because Defendants are covered by HIPAA (45 C.F.R. § 160.102), it is required to comply with the HIPAA Privacy Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule

[6] https://www.nbcsandiego.com/news/local/scripps-health-employees-regaining-access-to-internal-systems-hit-by-cyberattack-2/2619540/ (last accessed November 5, 2021).
[7] https://www.nbcsandiego.com/news/local/data-breach-at-uc-san-diego-health-some-employee-email-accounts-impacted/2670302/ (last accessed November 5, 2021).

("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

45. HIPAA's Privacy Rule or Standards for Privacy of Individually Identifiable Health Information establishes national standards for the protection of health information.

46. HIPAA's Privacy Rule or Security Standards for the Protection of Electronic Protected Health Information establishes a national set of security standards for protecting health information that is kept or transferred in electronic form.

47. HIPAA requires Defendants to "comply with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302.

48. "Electronic protected health information" is "individually identifiable health information … that is (i) transmitted by electronic media; maintained in electronic media." 45 C.F.R. § 160.103.

49. HIPAA's Security Rule requires Defendants to do the following:

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 by their workforce.

50. HIPAA also requires Defendants 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." 45 C.F.R. § 164.312(a)(1).

51. Moreover, the HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, requires Defendants to provide notice of the Data Breach to each affected individual "without unreasonable delay and in no case later than 60 days following discovery of the breach."

52. Defendants were also prohibited by the Federal Trade Commission Act (the "FTC Act") (15 U.S.C. § 45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission (the "FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. See, e.g., *FTC v. Wyndham Worldwide Corp*., 799 F.3d 236 (3d Cir. 2015).

53. In addition to its obligations under federal and state laws, Defendants owed a duty to Representative Plaintiff(s) and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PHI/PII in Defendants' possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendants owed a duty to Representative Plaintiff(s) and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that their computer systems, networks, and protocols adequately protected the PHI/PII of Representative Plaintiff(s) and Class Members.

54. Defendants owed a duty to Representative Plaintiff(s) and Class Members to design, maintain, and test their computer systems, servers, and networks to ensure that the PHI/PII in their possession was adequately secured and protected.

55. Defendants owed a duty to Representative Plaintiff(s) and Class Members to create and implement reasonable data security practices and procedures to protect the PHI/PII in their possession, including not sharing information with other/her/their entities who maintained sub-standard data security systems.

56. Defendants owed a duty to Representative Plaintiff(s) and Class Members to implement processes that would immediately detect a breach on their data security systems in a timely manner.

57. Defendants owed a duty to Representative Plaintiff(s) and Class Members to act upon data security warnings and alerts in a timely fashion.

58. Defendants owed a duty to Representative Plaintiff(s) and Class Members to disclose if their computer systems and data security practices were inadequate to safeguard individuals' PHI/PII and/or financial information from theft because such an inadequacy would be a material fact in the decision to entrust this PHI/PII and/or financial information to Defendants.

59. Defendants owed a duty of care to Representative Plaintiff(s) and Class Members because they were foreseeable and probable victims of any inadequate data security practices.

60. Defendants owed a duty to Representative Plaintiff(s) and Class Members to encrypt and/or more reliably encrypt Representative Plaintiff(s)' and Class Members' PHI/PII and monitor user behavior and activity in order to identity possible threats.

Value of the Relevant Sensitive Information

61. While the greater efficiency of electronic health records translates to cost savings for providers, it also comes with the risk of privacy breaches. These electronic health records contain a plethora of sensitive information (e.g., patient data, patient diagnosis, lab results, RX's, treatment plans) that is valuable to cyber criminals. One patient's complete record can be sold for hundreds of dollars on the dark web. As such, PHI/PII are valuable commodities for which a "cyber black market" exists in which criminals openly post stolen payment card numbers, Social Security numbers, and other personal information on a number of underground internet websites. Unsurprisingly, the healthcare industry is at high risk for and acutely affected by cyberattacks.

62. The high value of PHI/PII to criminals is further evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[8] Experian reports that a stolen credit or debit card number

[8] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed July 28, 2021).

can sell for $5 to $110 on the dark web.[9] Criminals can also purchase access to entire company data breaches from $999 to $4,995.[10]

63. Between 2005 and 2019, at least 249 million people were affected by health care data breaches.[11] Indeed, during 2019 alone, over 41 million healthcare records were exposed, stolen, or unlawfully disclosed in 505 data breaches.[12] In short, these sorts of data breaches are increasingly common, especially among healthcare systems, which account for 30.03% of overall health data breaches, according to cybersecurity firm Tenable.[13]

64. These criminal activities have and will result in devastating financial and personal losses to Representative Plaintiff(s) and Class Members. For example, it is believed that certain PHI/PII compromised in the 2017 Experian data breach was being used, three years later, by identity thieves to apply for COVID-19-related benefits in the state of Oklahoma. Such fraud will be an omnipresent threat for Representative Plaintiff(s) and Class Members for the rest of their lives. They will need to remain constantly vigilant.

65. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."

---

[9] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last accessed November 5, 2021).

[10] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed January 21, 2022).

[11] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7349636/#B5-healthcare-08-00133 (last accessed January 21, 2022).

[12] https://www.hipaajournal.com/december-2019-healthcare-data-breach-report/ (last accessed January 21, 2022).

[13] https://www.tenable.com/blog/healthcare-security-ransomware-plays-a-prominent-role-in-covid-19-era-breaches (last accessed January 21, 2022).

66. Identity thieves can use PHI/PII, such as that of Representative Plaintiff(s) and Class Members which Defendants failed to keep secure, to perpetrate a variety of crimes that harm victims. For instance, identity thieves may commit various types of government fraud such as immigration fraud, obtaining a driver's license or identification card in the victim's name but with another's picture, using the victim's information to obtain government benefits, or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund.

67. The ramifications of Defendants' failure to keep secure Representative Plaintiff(s)' and Class Members' PHI/PII are long lasting and severe. Once PHI/PII is stolen, particularly identification numbers, fraudulent use of that information and damage to victims may continue for years. Indeed, the PHI/PII and/or financial information of Representative Plaintiff(s) and Class Members was taken by hackers to engage in identity theft or to sell it to other criminals who will purchase the PHI/PII and/or financial information for that purpose. The fraudulent activity resulting from the Data Breach may not come to light for years.

68. There may be a time lag between when harm occurs versus when it is discovered, and also between when PHI/PII and/or financial information 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.[14]

69. The harm to Representative Plaintiff(s) and Class Members is especially acute given the nature of the leaked data. Medical identity theft is one of the most common, most expensive, and most difficult-to-prevent forms of identity theft. According to Kaiser Health News, "medical-related identity theft accounted for 43 percent of all identity thefts reported in the United

[14] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* http://www.gao.gov/new.items/d07737.pdf (last accessed January 21, 2022).

States in 2013," which is more than identity thefts involving banking and finance, the government and the military, or education.[15]

70. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[16]

71. When cyber criminals access financial information, health insurance information and other personally sensitive data—as they did here—there is no limit to the amount of fraud to which Defendants may have exposed Representative Plaintiff(s) and Class Members.

72. A study by Experian found that the average total cost of medical identity theft is "about $20,000" per incident, and that a majority of victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[17] Almost half of medical identity theft victims lose its healthcare coverage as a result of the incident, while nearly one-third saw its insurance premiums rise, and forty percent were never able to resolve its identity theft at all.[18]

73. And data breaches are preventable.[19] As Lucy Thompson wrote in the DATA BREACH AND ENCRYPTION HANDBOOK, "[i]n almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions."[20] She/he/they added that "[o]rganizations that collect, use, store, and share

---

[15] Michael Ollove, "The Rise of Medical Identity Theft in Healthcare," Kaiser Health News, Feb. 7, 2014, https://khn.org/news/rise-of-indentity-theft/ (last accessed January 21, 2022).
[16] *Id*.
[17] See Elinor Mills, "Study: Medical Identity Theft is Costly for Victims," CNET (Mar, 3, 2010), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/ (last accessed January 21, 2022).
[18] Id.; see also Healthcare Data Breach: What to Know About them and What to Do After One, EXPERIAN, https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/ (last accessed January 21, 2022).
[19] Lucy L. Thompson, "Despite the Alarming Trends, Data Breaches Are Preventable," *in* DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012)
[20] *Id.* at 17.

sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised . . . ."[21]

74. Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures … Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a *data breach never occurs*."[22]

75. Here, Defendants knew of the importance of safeguarding PHI/PII and of the foreseeable consequences that would occur if Representative Plaintiff(s)' and Class Members' PHI/PII was stolen, including the significant costs that would be placed on Representative Plaintiff(s) and Class Members as a result of a breach of this magnitude. As detailed above, Defendants are large, sophisticated organizations with the resources to deploy robust cybersecurity protocols. They knew, or should have known, that the development and use of such protocols were necessary to fulfill their statutory and common law duties to Representative Plaintiff(s) and Class Members. their failure to do so is, therefore, intentional, willful, reckless and/or grossly negligent.

76. Defendants disregarded the rights of Representative Plaintiff(s) and Class Members by, *inter alia*, (i) intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure that their network servers were protected against unauthorized intrusions; (ii) failing to disclose that they did not have adequately robust security protocols and training practices in place to adequately safeguard Representative Plaintiff(s)' and Class Members' PHI/PII and/or financial information; (iii) failing to take standard and reasonably available steps to prevent the Data Breach; (iv) concealing the existence and extent of the Data Breach for an unreasonable duration of time; and (v) failing to provide Representative Plaintiff(s) and Class Members prompt and accurate notice of the Data Breach.

Plaintiff David Underwood's Experience

77. Plaintiff David Underwood is a former patient of Defendant Hapy Bear Surgical Center, LLC.

---

[21] *Id.* at 28.
[22] *Id.*

78. As a condition of receiving services from Defendants, Plaintiff Underwood was required to provide his private information to Defendant, including his full name, address, medical information, health insurance information, social security number, and driver's license number.

79. At the time of the Data Breach, Defendants retained Plaintiff Underwood's PHI/PII in its system.

80. Plaintiff Underwood is very careful about sharing his sensitive PHI/PII. Plaintiff stores any documents containing his PHI/PII in a safe and secure location. He has never knowingly transmitted unencrypted sensitive PHI/PII over the internet or any other unsecured source. Plaintiff Underwood would not have entrusted his PHI/PII to Defendant had he known of Defendant's lax data security policies.

81. Plaintiff Underwood received the Notice Letter, by U.S. mail, directly from Defendant, dated April 11, 2024. According to the Notice Letter, Plaintiff's Private Information was improperly accessed and obtained by unauthorized third parties, including his full name, address, medical information, health insurance information, social security number, and driver's license number.

82. As a result of the Data Breach, and at the direction of Defendant's Notice Letter, Plaintiff Underwood made reasonable efforts to mitigate the impact of the Data Breach, including researching and verifying the legitimacy of the Data Breach upon receiving the Notice Letter, changing passwords and resecuring his own computer network, and contacting companies regarding suspicious activity on his accounts. Plaintiff Underwood has spent significant time dealing with the Data Breach—valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

83. Plaintiff Underwood further suffered actual injury in the form of experiencing an increase in spam phone calls, text messages, and emails, upon information and belief, was caused

by the Data Breach.

84. The Data Breach has caused Plaintiff Underwood to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendants have still not fully informed him of key details about the Data Breach's occurrence.

85. As a result of the Data Breach, Plaintiff Underwood anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

86. As a result of the Data Breach, Plaintiff Underwood is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

87. Plaintiff Underwood has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

CLASS ACTION ALLEGATIONS

88. Representative Plaintiff brings this action individually and on behalf of all persons similarly situated and proximately damaged by Defendants' conduct including, but not necessarily limited to, the following Plaintiff Class:

> "All individuals within the United States of America whose PHI/PII was exposed to unauthorized third parties as a result of the data breach experienced by Defendant on December 27, 2023."

89. Excluded from the Classes are the following individuals and/or entities: Defendants and Defendants' parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendants have a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to its departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as its immediate family members.

90. Also, in the alternative, Representative Plaintiff(s) request additional Subclasses as necessary based on the types of PII/PHI that were compromised.

91. Representative Plaintiff(s) reserve the right to amend the above definition or to propose subclasses in subsequent pleadings and motions for class certification.

92. This action has been brought and may properly be maintained as a class action under California Code of Civil Procedure § 382 because there is a well-defined community of interest in the litigation and the proposed class is easily ascertainable.

a. Numerosity: A class action is the only available method for the fair and efficient adjudication of this controversy. The members of the Plaintiff Class are so numerous that joinder of all members is impractical, if not impossible. Representative Plaintiff is informed and believes and, on that basis, alleges that the total number of Class Members is in the thousands of individuals. Membership in the Class will be determined by analysis of Defendants' records.

b. Commonality: Representative Plaintiff and Class Members share a community of interests in that there are numerous common questions and issues of fact and law which predominate over any questions and issues solely affecting individual members, including, but not necessarily limited to:

1) Whether Defendants engaged in the wrongful conduct alleged herein;

2) Whether Defendants had a legal duty to Representative Plaintiff and Class Members to exercise due care in collecting, storing, using, and/or safeguarding their PII;

3) Whether Defendants knew or should have known of the susceptibility of Defendants' data security systems to a data breach;

4) Whether Defendants' security procedures and practices to protect their systems were reasonable in light of the measures recommended by data security experts;

5) Whether Defendants' failure to implement adequate data security measures, including the sharing of Representative Plaintiff's and Class Members' PHI/PII allowed the Data Breach to occur and/or worsened its effects;

6) Whether Defendants failed to comply with their own policies and applicable laws, regulations, and industry standards relating to data security;

7) Whether Defendants adequately, promptly, and accurately informed Representative Plaintiff and Class Members that their PHI/PII had been compromised;

8) How and when Defendants actually learned of the Data Breach;

9) Whether Defendants failed to adequately respond to the Data Breach, including failing to investigate it diligently and notify affected individuals in the most expedient time possible and without unreasonable delay, and whether this caused damages to Representative Plaintiff and Class Members;

10) Whether Defendants' conduct, including their failure to act, resulted in or was the proximate cause of the breach of these systems, resulting in the loss of the PHI/PII of Representative Plaintiff and Class Members;

11) Whether Defendants adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

12) Whether Defendants' conduct, including their failure to act, resulted in or was the proximate cause of the Data Breach and/or damages flowing therefrom;

13) Whether Defendants' actions alleged herein constitute gross negligence and whether the negligence/recklessness of any one or more individual(s) can be imputed to Defendants;

14) Whether Defendants engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PHI/PII of Representative Plaintiff and Class Members;

15) Whether Representative Plaintiff and Class Members are entitled to actual and/or statutory damages and/or whether injunctive, corrective, and/or declaratory relief and/or an accounting is/are appropriate as a result of Defendants' wrongful conduct and, if so, what is necessary to redress the imminent and currently ongoing harm faced by Representative Plaintiff, Class Members, and the general public;

16) Whether Representative Plaintiff and Class Members are entitled to restitution as a result of Defendants' wrongful conduct;

17) Whether Defendants continue to breach duties to Representative Plaintiff and Class Members.

c. Typicality: Representative Plaintiff's claims are typical of the claims of the Plaintiff Class. Representative Plaintiff and all members of the Plaintiff Class sustained damages arising out of and caused by Defendants' common course of conduct in violation of law, as alleged herein. The same event and conduct that gave rise to Representative Plaintiff's claims are identical to those that give rise to the claims of every Class Member because Representative Plaintiff and each Class Member who had his/her sensitive PHI/PII and/or financial information compromised in the same way by the same conduct of Defendants. Representative Plaintiff and all Class

Members face the identical threats resulting from the breach of his/her PHI/PII and/or financial information without the protection of encryption and adequate monitoring of user behavior and activity necessary to identity those threats.

d. Adequacy of Representation: Representative Plaintiff is an adequate representative of the Plaintiff Class in that Representative Plaintiff has the same interest in the litigation of this case as the remaining Class Members, is committed to vigorous prosecution of this case and has retained competent counsel who are experienced in conducting litigation of this nature. Representative Plaintiff is not subject to any individual defenses unique from those conceivably applicable to other Class Members or the class in its entirety. Representative Plaintiff anticipates no management difficulties in this litigation. Representative Plaintiff and proposed class counsel will fairly and adequately protect the interests of all Class Members.

Superiority of Class Action: The damages suffered by individual Class Members, are significant, but may be small relative to the enormous expense of individual litigation by each member. This makes or may make it impractical for members of the Plaintiff Class to seek redress individually for the wrongful conduct alleged herein. Even if Class Members could afford such individual litigation, the court system could not. Should separate actions be brought or be required to be brought, by each individual member of the Plaintiff Class, the resulting multiplicity of lawsuits would cause undue hardship and expense for the Court and the litigants. The prosecution of separate actions would also create a risk of inconsistent rulings which might be dispositive of the interests of other Class Members who are not parties to the adjudications and/or may substantially impede their ability to adequately protect their interests. Individualized litigation increases the delay and expense to all parties, and to the court system, presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties and provides benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

93. Class certification is proper because the questions raised by this Complaint are of common or general interest affecting numerous persons, such that it is impracticable to bring all Class Members before the Court.

94. This class action is also appropriate for certification because Defendants have acted and/or have refused to act on grounds generally applicable to the Class(es), thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward Class Members and making final injunctive relief appropriate with respect to the Class(es) in their entireties. Defendants' policies/practices challenged herein apply to and affect Class Members

uniformly and Representative Plaintiff's challenge of these policies/practices and conduct hinges on Defendants' conduct with respect to the Classes in their entireties, not on facts or law applicable only to the Representative Plaintiff.

95. Unless a Class-wide injunction is issued, Defendants' violations may continue, and Defendants may continue to act unlawfully as set forth in this Complaint.

FIRST CAUSE OF ACTION
Negligence

96. Each and every allegation of the preceding paragraphs is incorporated in this cause of action with the same force and effect as though fully set forth herein.

97. At all times herein relevant, Defendants owed Representative Plaintiff and Class Members a duty of care, *inter alia*, to act with reasonable care to secure and safeguard their PHI/PII and to use commercially reasonable methods to do so. Defendants took on this obligation upon accepting and storing the PHI/PII of Representative Plaintiff and Class Members in their computer systems and on their networks.

98. Among these duties, Defendants were expected:

a. to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting the PHI/PII in their possession;

b. to protect Representative Plaintiff's and Class Members' PHI/PII using reasonable and adequate security procedures and systems that were/are compliant with industry-standard practices;

c. to implement processes to quickly detect the Data Breach and to timely act on warnings about data breaches; and

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

99. Defendants knew, or should have known, that the PHI/PII was private and confidential and should be protected as private and confidential and, thus, Defendants owed a duty of care not to subject Representative Plaintiff and Class Members to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices.

100. Defendants knew, or should have known, of the risks inherent in collecting and storing PII, the vulnerabilities of their data security systems, and the importance of adequate security. Defendants knew about numerous, well-publicized data breaches.

101. Defendants knew, or should have known, that their data systems and networks did not adequately safeguard Representative Plaintiff's and Class Members' PII.

102. Only Defendants were in the position to ensure that their systems and protocols were sufficient to protect the PHI/PII Representative Plaintiff and Class Members had entrusted to it.

103. Defendants breached their duties to Representative Plaintiff and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard the PHI/PII of Representative Plaintiff and Class Members.

104. Because Defendants knew that a breach of their systems could damage thousands of individuals, including Representative Plaintiff and Class Members, Defendants had a duty to adequately protect their data systems and the PHI/PII contained thereon.

105. Representative Plaintiff's and Class Members' willingness to entrust Defendants with their PHI/PII was predicated on the understanding that Defendants would take adequate security precautions. Moreover, only Defendants had the ability to protect their systems and the PHI/PII they stored on them from attack. Thus, Defendants had a special relationship with Representative Plaintiff and Class Members.

106. Defendants also had independent duties under state and federal laws that required Defendants to reasonably safeguard Representative Plaintiff's and Class Members' PHI/PII and promptly notify them about the Data Breach. These "independent duties" are untethered to any contract between Defendants and Representative Plaintiff and/or the remaining Class Members.

107. Defendants breached their general duty of care to Representative Plaintiff and Class Members in, but not necessarily limited to, the following ways:

a. by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard the PHI/PII of Representative Plaintiff and Class Members;

b. by failing to timely and accurately disclose that Representative Plaintiff's and Class Members' PHI/PII had been improperly acquired or accessed;

c. by failing to adequately protect and safeguard the PHI/PII by knowingly disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured PII;

d. by failing to provide adequate supervision and oversight of the PHI/PII with which they were and are entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted an unknown third-party to gather PHI/PII of Representative Plaintiff and Class Members, misuse the PHI/PII and intentionally disclose it to others without consent.

e. by failing to adequately train their employees to not store PHI/PII longer than absolutely necessary;

f. by failing to consistently enforce security policies aimed at protecting Representative Plaintiff's and the Class Members' PII;

g. by failing to implement processes to quickly detect data breaches, security incidents, or intrusions; and

h. by failing to encrypt Representative Plaintiff's and Class Members' PHI/PII and monitor user behavior and activity in order to identify possible threats.

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

109. As a proximate and foreseeable result of Defendants' grossly negligent conduct, Representative Plaintiff and Class Members have suffered damages and are at imminent risk of additional harms and damages (as alleged above).

110. The law further imposes an affirmative duty on Defendants to timely disclose the unauthorized access and theft of the PHI/PII to Representative Plaintiff and Class Members so that they could and/or still can take appropriate measures to mitigate damages, protect against adverse consequences and thwart future misuse of their PII.

111. Defendants breached their duty to notify Representative Plaintiff and Class Members of the unauthorized access by waiting months after learning of the Data Breach to notify Representative Plaintiff and Class Members and then by failing and continuing to fail to provide Representative Plaintiff and Class Members sufficient information regarding the breach. To date, Defendants have not provided sufficient information to Representative Plaintiff and Class

Members regarding the extent of the unauthorized access and continues to breach their disclosure obligations to Representative Plaintiff and Class Members.

112. Further, through their failure to provide timely and clear notification of the Data Breach to Representative Plaintiff and Class Members, Defendants prevented Representative Plaintiff and Class Members from taking meaningful, proactive steps to secure their PII.

113. There is a close causal connection between Defendants' failure to implement security measures to protect the PHI/PII of Representative Plaintiff and Class Members and the harm suffered, or risk of imminent harm suffered by Representative Plaintiff and Class Members. Representative Plaintiff's and Class Members' PHI/PII was accessed as the proximate result of Defendants' failure to exercise reasonable care in safeguarding such PHI/PII by adopting, implementing, and maintaining appropriate security measures.

114. Defendants' wrongful actions, inactions, and omissions constituted (and continue to constitute) common law negligence.

115. The damages Representative Plaintiff and Class Members have suffered (as alleged above) and will suffer were and are the direct and proximate result of Defendants' grossly negligent conduct.

116. Additionally, 15 U.S.C. §45 (FTC Act, Section 5) prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendants, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendants' duty in this regard.

117. Defendants violated 15 U.S.C. §45 by failing to use reasonable measures to protect PHI/PII and not complying with applicable industry standards, as described in detail herein. Defendants' conduct was particularly unreasonable given the nature and amount of PHI/PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Representative Plaintiff and Class Members.

118. As a direct and proximate result of Defendants' negligence and negligence *per se*, Representative 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 of how their PHI/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 embarrassment and identity theft; (vi) the continued risk to their PII, which may remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect Representative Plaintiff's and Class Members' PHI/PII in their continued possession; (vii) and future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PHI/PII compromised as a result of the Data Breach for the remainder of the lives of Representative Plaintiff and Class Members.

119. As a direct and proximate result of Defendants' negligence and negligence *per se*, Representative Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

120. Additionally, as a direct and proximate result of Defendants' negligence and negligence *per se*, Representative Plaintiff and Class Members have suffered and will suffer the continued risks of exposure of their PII, which remain in Defendants' possession and are subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PHI/PII in their continued possession.

SECOND CAUSE OF ACTION
Breach of Implied Contract

121. Each and every allegation of the preceding paragraphs is incorporated in this cause of action with the same force and effect as though fully set forth herein.

122. Through their course of conduct, Defendants, Representative Plaintiff, and Class Members entered into implied contracts for Defendants to implement data security adequate to safeguard and protect the privacy of Representative Plaintiff's and Class Members' PII.

123. As part of this contract, Defendants required Representative Plaintiff and Class Members to provide and entrust to Defendant, *inter alia*, names, addresses, dates of birth, Social Security numbers, driver's license numbers, financial account information, health insurance plan member ID's, claims data, and clinical information.

124. Defendants solicited and invited Representative Plaintiff and Class Members to provide their PHI/PII as part of Defendants' regular business practices. Representative Plaintiff and Class Members accepted Defendants' offers and provided their PHI/PII thereto.

125. As a condition of being patients thereof, Representative Plaintiff and Class Members provided and entrusted their PHI/PII to Defendants. In so doing, Representative Plaintiff and Class Members entered into implied contracts with Defendants by which Defendants agreed to safeguard and protect such non-public information, to keep such information secure and confidential, and to timely and accurately notify Representative Plaintiff and Class Members if their data had been breached and compromised or stolen.

126. A meeting of the minds occurred when Representative Plaintiff and Class Members agreed to, and did, provide their PHI/PII to Defendants, in exchange for, amongst other things, the protection of their PII.

127. Representative Plaintiff and Class Members fully performed their obligations under the implied contracts with Defendants.

128. Defendants breached the implied contracts they made with Representative Plaintiff and Class Members by failing to safeguard and protect their PHI/PII and by failing to provide timely and accurate notice to them that their PHI/PII was compromised as a result of the Data Breach.

129. As a direct and proximate result of Defendants' above-described breach of implied contract, Representative Plaintiff and Class Members have suffered (and will continue to suffer) (a) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting

in monetary loss and economic harm; (b) actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; (c) loss of the confidentiality of the stolen confidential data; (d) the illegal sale of the compromised data on the dark web; (e) lost work time; and (f) other economic and non-economic harm.

THIRD CAUSE OF ACTION
Violation of the Confidentiality of Medical Information Act
(Cal. Civ. Code §56, *et seq*.)

130. Each and every allegation of the preceding paragraphs is incorporated in this cause of action with the same force and effect as though fully set forth herein.

131. Under the CMIA, California Civil Code §56.05(k), Representative Plaintiff and Class Members (except employees of Defendants whose records may have been accessed) are deemed "patients."

132. As defined in the CMIA, California Civil Code §56.05(j), Defendants disclosed "medical information" to unauthorized persons without obtaining consent, in violation of §56.10(a). Defendants' misconduct, including failure to adequately detect, protect, and prevent unauthorized disclosure, directly resulted in the unauthorized disclosure of Representative Plaintiff's and Class Members' PHI/PII to unauthorized persons. This information was subsequently viewed by unauthorized third parties as a direct result of this disclosure.

133. Defendants' misconduct, including protecting and preserving the confidential integrity of their clients'/customers' PHI/PII, resulted in unauthorized disclosure of sensitive and confidential PHI/PII that belongs to Representative Plaintiff and Class Members to unauthorized persons, breaching the confidentiality of that information, thereby violating California Civil Code §§ 56.06 and 56.101(a).

134. Representative Plaintiff and Class Members have all been and continue to be harmed as a direct, foreseeable, and proximate result of Defendants' breach because Representative Plaintiff and Class Members face, now and in the future, an imminent threat of identity theft, fraud, and for ransom demands. They must now spend time, effort and money to constantly monitor their accounts and credit to surveille for any fraudulent activity.

135. Representative Plaintiff and Class Members were injured and have suffered damages, as described above, from Defendants' illegal disclosure and negligent release of their PHI/PII in violation of Cal. Civ. Code §§ 56.10 and 56.101 and, therefore, seek relief under Civ. Code §§ 56.35 and 56.36, including actual damages, nominal statutory damages, punitive damages, injunctive relief, and attorneys' fees and costs.

FOURTH CAUSE OF ACTION
Unfair Business Practices
(Cal. Bus. & Prof. Code, §17200, *et seq*.)

136. Each and every allegation of the preceding paragraphs is incorporated in this cause of action with the same force and effect as though fully set forth herein.

137. Representative Plaintiff and Class Members further bring this cause of action, seeking equitable and statutory relief to stop the misconduct of Defendants, as complained of herein.

138. Defendants have engaged in unfair competition within the meaning of California Business & Professions Code §§17200, *et seq.*, because their conduct was/is unlawful, unfair, and/or fraudulent, as herein alleged.

139. Representative Plaintiff, the Class Members, and Defendants are each a "person" or "persons" within the meaning of § 17201 of the California Unfair Competition Law ("UCL").

140. The knowing conduct of Defendants, as alleged herein, constitutes an unlawful and/or fraudulent business practice, as set forth in California Business & Professions Code §§17200-17208. Specifically, Defendants conducted business activities while failing to comply with the legal mandates cited herein. Such violations include, but are not necessarily limited to:

a. failure to maintain adequate computer systems and data security practices to safeguard PII;

b. failure to disclose that their computer systems and data security practices were inadequate to safeguard PHI/PII from theft;

c. failure to timely and accurately disclose the Data Breach to Representative Plaintiff and Class Members;

d. continued acceptance of PHI/PII and storage of other personal information after Defendants knew or should have known of the security vulnerabilities of the systems that were exploited in the Data Breach; and

e. continued acceptance of PHI/PII and storage of other personal information after Defendants knew or should have known of the Data Breach and before they allegedly remediated the Data Breach.

141. Defendants knew or should have known that their computer systems and data security practices were inadequate to safeguard the PHI/PII of Representative Plaintiff and Class Members, deter hackers, and detect a breach within a reasonable time and that the risk of a data breach was highly likely.

142. In engaging in these unlawful business practices, Defendants have enjoyed an advantage over their competition and a resultant disadvantage to the public and Class Members.

143. Defendants' knowing failure to adopt policies in accordance with and/or adhere to these laws, all of which are binding upon and burdensome to Defendants' competitors, engenders an unfair competitive advantage for Defendants, thereby constituting an unfair business practice, as set forth in California Business & Professions Code §§17200-17208.

144. Defendants have clearly established a policy of accepting a certain amount of collateral damage, as represented by the damages to Representative Plaintiff and Class Members herein alleged, as incidental to their business operations, rather than accept the alternative costs of full compliance with fair, lawful, and honest business practices ordinarily borne by responsible competitors of Defendants and as set forth in legislation and the judicial record.

145. The UCL is, by its express terms, a cumulative remedy, such that remedies under its provisions can be awarded in addition to those provided under separate statutory schemes and/or common law remedies, such as those alleged in the other causes of action in this Complaint. *See* Cal. Bus. & Prof. Code § 17205.

146. Representative Plaintiff and Class Members request that this Court enter such orders or judgments as may be necessary to enjoin Defendants from continuing their unfair, unlawful, and/or deceptive practices and to restore to Representative Plaintiff and Class Members any money Defendants acquired by unfair competition, including restitution and/or equitable relief, including disgorgement of ill-gotten gains, refunds of moneys, interest, reasonable attorneys'

fees, and the costs of prosecuting this class action, as well as any and all other relief that may be available at law or equity.

FIFTH CAUSE OF ACTION
Unjust Enrichment

147. Each and every allegation of the preceding paragraphs is incorporated in this cause of action with the same force and effect as though fully set forth herein.

148. By their wrongful acts and omissions described herein, Defendants have obtained a benefit by unduly taking advantage of Representative Plaintiff and Class Members.

149. Defendants, prior to and at the time Representative Plaintiff and Class Members entrusted their PHI/PII to Defendants for the purpose of purchasing services from Defendants, caused Representative Plaintiff and Class Members to reasonably believe that Defendants would keep such PHI/PII secure.

150. Defendants were aware, or should have been aware, that reasonable consumers would have wanted their PHI/PII kept secure and would not have contracted with Defendants, directly or indirectly, had they known that Defendants' information systems were sub-standard for that purpose.

151. Defendants were also aware that if the substandard condition of and vulnerabilities in their information systems were disclosed, it would negatively affect Representative Plaintiff's and Class Members' decisions to engage with Defendants.

152. Defendants failed to disclose facts pertaining to their substandard information systems, defects, and vulnerabilities therein before Representative Plaintiff and Class Members made their decisions to make purchases, engage in commerce therewith, and seek services or information. Instead, Defendants suppressed and concealed such information. By concealing and suppressing that information, Defendants denied Representative Plaintiff and Class Members the ability to make a rational and informed purchasing decision and took undue advantage of Representative Plaintiff and Class Members.

153. Defendants were unjustly enriched at the expense of Representative Plaintiff and Class Members. Defendants received profits, benefits, and compensation, in part, at the expense of

Representative Plaintiff and Class Members. By contrast, Representative Plaintiff and Class Members did not receive the benefit of their bargain because they paid for services that did not satisfy the purposes for which they bought/sought them.

154. Since Defendants' profits, benefits, and other compensation were obtained by improper means, Defendants are not legally or equitably entitled to retain any of the benefits, compensation or profits they realized from these transactions.

155. Representative Plaintiff and Class Members seek an Order of this Court requiring Defendants to refund, disgorge, and pay as restitution any profits, benefits and other compensation obtained by Defendants from their wrongful conduct and/or the establishment of a constructive trust from which Representative Plaintiff and Class Members may seek restitution.

RELIEF SOUGHT

WHEREFORE, Representative Plaintiff, individually, as well as on behalf of each member of the proposed Class(es), respectfully requests that the Court enter judgment in Representative Plaintiff's favor and for the following specific relief against Defendants as follows:

1. That the Court declare, adjudge, and decree that this action is a proper class action and certify the proposed class and/or any other appropriate subclasses under California Code of Civil Procedure § 382;

2. For an award of damages, including actual, nominal, consequential, statutory, and punitive damages, as allowed by law in an amount to be determined;

3. That the Court enjoin Defendants, ordering them to cease and desist from unlawful activities in further violation of California Business and Professions Code §17200, *et seq.*;

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

5. For injunctive relief requested by Representative Plaintiff and Class Members, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Representative Plaintiff and Class Members, including but not limited to an Order:

a. prohibiting Defendants from engaging in the wrongful and unlawful acts described herein;

b. requiring Defendants to protect, including through encryption, all data collected through the course of business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

c. requiring Defendants to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of Representative Plaintiff's and Class Members' PII;

d. requiring Defendants to engage independent third-party security auditors and internal personnel to run automated security monitoring, simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis;

e. prohibiting Defendants from maintaining Representative Plaintiff's and Class Members' PHI/PII on a cloud-based database;

f. requiring Defendants to segment data by creating firewalls and access controls so that, if one area of Defendants networks are compromised, hackers cannot gain access to other portions of Defendants' systems;

g. requiring Defendants to conduct regular database scanning and securing checks;

h. requiring Defendants to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling PII, as well as protecting the PHI/PII of Representative Plaintiff and Class Members;

i. requiring Defendants to implement a system of tests to assess their respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendants' policies, programs, and systems for protecting PII;

j. requiring Defendants to implement, maintain, review, and revise as necessary a threat management program to appropriately monitor Defendants' networks for internal and external threats, and assess whether monitoring tools are properly configured, tested, and updated;

k. requiring Defendants to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves.

6. For prejudgment interest on all amounts awarded, at the prevailing legal rate;

7. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

8. For all other Orders, findings, and determinations sought in this Complaint.

JURY DEMAND

Representative Plaintiff, individually and on behalf of the Plaintiff Class, hereby demands a trial by jury for all issues triable by jury.

Dated: April 15, 2024

By: _____

Daniel Srourian, Esq. [SBN 285678]
SROURIAN LAW FIRM, P.C.
3435 Wilshire Blvd., Suite 1710
Los Angeles, CA 90010
Telephone: (213) 474-3800
Fax: (213) 471-4160
Email: daniel@slfla.com

Attorneys for Representative Plaintiff(s) and the Plaintiff Class(es)

EXHIBIT A

Hapy Bear Surge
c/o Cyberscout
PO Box 1286
Dearborn, MI 48

PJU2KW004001
UNDERWOOD

ClassAction.org