UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF FLORIDA
ORLANDO DIVISION

LORI GRADER and DARYL SWANSON, individually and on behalf of all others similarly situated, Plaintiffs, v. BIOPLUS SPECIALTY PHARMACY SERVICES, LLC., Defendant.	Case No.: _____ **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Lori Grader ("Plaintiff Grader") and Plaintiff Daryl Swanson ("Plaintiff Swanson") (collectively "Plaintiffs"), individually and on behalf of all others similarly situated ("Class Members"), bring this Class Action Complaint against BioPlus Specialty Pharmacy Services, LLC. ("BioPlus" or "Defendant"). Plaintiffs allege upon personal knowledge as to their own actions and the investigation of their counsel, and upon information and belief as to all other matters, as follows:

INTRODUCTION

1. Plaintiffs bring this Class Action Complaint against Defendant for its failure to adequately secure and safeguard electronically stored, personally identifiable information ("PII") and protected health information ("PHI"), including,

without limitation, Social Security numbers, full names, birthdates,[1] and prescription information.[2]

2. BioPlus provides specialty pharmacy services.[3] Its services include infusion services.

3. Individuals entrust Defendant with an extensive amount of their PII and PHI. Defendant claims that it understands the importance of protecting such information, and that "privacy of patients' health information is very important to . . . us."[4]

4. Despite that proclamation, however, on or before November 11, 2021, Defendant learned that an unauthorized actor breached its system and gained access on October 25, 2021 and acquired electronic files containing the PII and PHI of Defendant's customers, including Plaintiffs' and Class Members' data (the "Data Breach"). The data included, at least, Plaintiffs' and Class Members' Social Security numbers, medical record number, current/former member ID number, claims

[1] Personally identifiable information 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.

[2] Health information, including diagnoses, treatment information, medical test results, and prescription information, is considered protected health information under the Health Insurance Portability and Accountability Act ("HIPAA"). *See* https://www.cdc.gov/phlp/publications/topic/hipaa.html#one.

[3] Exhibit A (*Notice of Data Event to the Washington State Attorney General*, dated May 5, 2021, also available at: https://agportal-s3bucket.s3.amazonaws.com/Data_Breach/NECNetworksDbaCaptureRx.2021-05-05.pdf.)

[4] https://bioplusrx.com/privacy-policy/ (last visited Jan. 25, 2022)

information, diagnosis information, names, dates of birth, prescription information, and address.

5. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' PII and PHI, Defendant assumed legal and equitable duties to those individuals.

6. The exposed PII and PHI of Plaintiffs and Class Members can be sold on the dark web. Hackers can access and then offer for sale the unencrypted, unredacted PII and PHI to criminals. Plaintiffs and Class Members face a present and immediate lifetime risk of identity theft, which is heightened here by the loss of their Social Security numbers, birthdates, and specific medical treatment information in the form of prescription information.

7. This PII and PHI was compromised due to Defendant's negligent and/or careless acts and omissions and the failure to protect the PII and PHI of Plaintiffs and Class Members, such as implementing basic security practices like encryption of highly sensitive information and deleting old information that is no longer needed.

8. Plaintiffs bring this action on behalf of all persons whose PII and PHI was compromised as a result of Defendant's failure to: (i) adequately protect the PII and PHI of Plaintiffs and Class Members; (ii) warn Plaintiffs and Class Members of their inadequate information security practices; and (iii) avoid sharing the PII and

PHI of Plaintiffs and Class Members without adequate safeguards. Defendant's conduct amounts to negligence and violates federal and state statutes.

9. Plaintiffs and Class Members have suffered injury as a result of Defendant's conduct. These injuries include: (i) lost or diminished value of PII and PHI; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their PII and PHI; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time, and (iv) the present and immediate risk to their PII and PHI, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) may remain backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII and PHI.

10. Defendant disregarded the rights of Plaintiffs and Class Members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that Plaintiffs' and Class Members' PII and PHI 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 PII and PHI of Plaintiffs and Class Members was compromised

through disclosure to an unknown and unauthorized criminal third party. Plaintiffs and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

PARTIES

Plaintiff Lori Grader

11. Plaintiff Lori Grader is a resident and citizen the State of Washington and intends to remain domiciled in and a citizen of the State of Washington.

12. Plaintiff Grader received a letter dated December 10, 2021 from Defendant concerning the Data Breach. The letter stated that her name, address, date of birth, Social Security number, medical record number, current/former health plan member ID number, claims information, diagnosis, and/or prescription information were exposed in the Data Breach.

13. Recognizing the substantial risk Plaintiff Grader faces, Defendant provided her a one-year subscription to a credit monitoring service. However, she was forced to spend time signing up for this service. Moreover, she will be forced to incur costs to maintain this service after her subscription expires in one year and intends on extending it for at least an additional two years.

14. Since learning of the Data Breach, Plaintiff Grader reviews her bank statements and credit cards at a more frequent interval than she did previously. She

has also spent significant time speaking with her bank regarding her concerns about the Data Breach.

15. The Data Breach has caused Plaintiff Grader to suffer significant fear, anxiety, and stress. She has lost a lot of sleep thinking about all the ways the Sensitive Information that was exposed can be used to commit fraud and identity theft.

16. Plaintiff Grader plans on taking additional time-consuming, yet necessary, steps to help mitigate the harm caused by the Data Breach, such as implementing credit freezes, monitoring her credit and identity, and checking her financial accounts.

Plaintiff Daryl Swanson

17. Plaintiff Daryl Swanson is a resident and citizen the State of Louisiana and intends to remain domiciled in and a citizen of the State of Louisiana.

18. Plaintiff Swanson received a letter dated December 10, 2021 from Defendant concerning the Data Breach. The letter stated that his name, address, date of birth, Social Security number, medical record number, current/former health plan member ID number, claims information, diagnosis, and/or prescription information were exposed in the Data Breach.

19. Recognizing the substantial risk Plaintiff Swanson faces, Defendant provided him a one-year subscription to a credit monitoring service. However, he

was forced to spend time signing up for this service. Moreover, he will be forced to incur costs to maintain this service after his subscription expires in one year and intends on extending it for at least an additional two years.

20. Since learning of the Data Breach, Plaintiff Swanson reviews his bank statements and credit cards at a more frequent interval than he did previously. He has also spent significant time speaking with his bank regarding his concerns about the Data Breach.

21. As a result of the Data Breach, Plaintiff Swanson now experiences spam phone calls that are designed to obtain more information from him.

22. The Data Breach has caused Plaintiff Swanson to suffer significant fear, anxiety, and stress. He has lost a lot of sleep thinking about all the ways the Sensitive Information that was exposed can be used to commit fraud and identity theft.

23. Plaintiff Swanson plans on taking additional time-consuming, yet necessary, steps to help mitigate the harm caused by the Data Breach, such as implementing credit freezes, monitoring his credit and identity, and checking his financial accounts.

Defendant BioPlus

24. Defendant BioPlus is a limited liability company organized in the State of Florida. It is headquartered in Altamonte Springs, Florida.

25. According to one of its recent business filing with the Florida Secretary of State, BioPlus's principal place of business is in this District and it, as an LLC, has three total members: (1) Stephen C. Vogt (manager member); (2) Hugh Stephen Garner (manager member); and (3) BioPlus Parent, LLC (authorized member). Member Stephen C. Vogt, an individual is domiciled in the State of Florida, a citizen of the State of Florida, and intends to remain a citizen of Florida with his permanent residence located at 1711 Barcelona Way, Winter Park, FL 32789-5616 – a property that carries a Homestead Exemption for 2022. Member Hugh Stephen Garner is domiciled in the State of Florida, a citizen of the State of Florida, and intends to remain in Florida with his permanent residence located at 720 Via Bella, Winter Park, FL 32789-2718 – a property that carries a Homestead Exemption for 2022. Authorized Member BioPlus Parent, LLC, is a Delaware business entity, with a single member – John Figueroa. Mr. Figueroa is a resident and citizen of the State of Washington and intends to remain a citizen of the State of Washington.

26. BioPlus advertises itself as its patients' "24/7 partner in health." It helps provide medications and individual therapeutic care plans to help patients manage conditions like hepatitis, Crohn's disease, multiple sclerosis, rheumatoid arthritis, psoriasis, psoriatic arthritis, and cancer. This includes online services, which provide

patients "expert advice on how to best manage [their] health and keep [them] feeling better."[5]

27. All of Plaintiffs' claims stated herein are asserted against Defendant and any of their owners, predecessors, successors, subsidiaries, agents and/or assigns.

JURISDICTION AND VENUE

28. This Court has original jurisdiction under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2), because this is a putative class action involving more than 100 Class Members and because the amount in controversy exceeds $5,000,000, exclusive of interests and costs. Moreover, Plaintiff Swanson is a citizen of the State of Louisiana and Defendant is a citizen of the State of Florida and the State of Washington. Therefore, minimal diversity under CAFA exists because Defendant as an LLC is a citizen of the State of Florida and the State of Washington, and a Plaintiff is a citizen of the State of Louisiana.

29. This Court has general personal jurisdiction over Defendant because Defendant is organized in Florida and has its principal place of business in Altamonte Springs, Florida.

30. Venue is proper in this District pursuant to 28 U.S.C. §§ 1391(a)(2), 1391(b)(2), and 1391(c)(2) as a substantial part of the events giving rise to the claims

[5] https://bioplusrx.com/patients/personalized-support/ (last visited Jan. 25, 2022)

emanated from activities within this District, and Defendant conducts substantial business in this District.

FACTUAL ALLEGATIONS

Background

31. Defendant requires the exchange of PII and PHI belonging to Plaintiffs and Class Members to provide services to these individuals. This sensitive and confidential PII and PHI, including, but not limited to, Social Security numbers, full names, and birthdates, is static and does not change, and can be used to commit myriad identity crimes. The PHI involved includes, but is not limited to, medical record number, current/former member ID number, claims information, prescription information, and diagnosis information is also sensitive and confidential, and is protected, private medical treatment information that divulges not only the types of pharmaceuticals Plaintiffs and Class Members were prescribed, but also the underlying mental or physical diagnoses.

32. Plaintiffs and Class Members relied on the sophistication of Defendant to keep their PII and PHI confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Plaintiffs and Class Members demand security to safeguard their PII and PHI.

33. Defendant had a duty to adopt reasonable measures to protect Plaintiffs'

and Class Members' PII and PHI from involuntary disclosure to third parties, such as encryption,[6] deleting information that is no longer needed, and other security measures, which are outlined below.

The Data Breach

34. On or about December 10, 2021, Defendant announced that they experienced the Data Breach. Defendant sent notice letters to various States' Attorneys General and to individuals impacted by the Data Breach. [7] The Notice to Plaintiffs Grader and Swanson, for example, stated that "on November 11, 2021 [BioPlus] identified suspicious activity on [their] IT network . . . We also launched an investigation with the assistance of a third-party forensic firm and notified law enforcement."[8]

35. Also, in the notice to impacted individuals, Defendant stated:

> Through our investigation, we determined that an unauthorized party gained access to our network between October 25, 2021 and November 11, 2021. During that time, the unauthorized party accessed files that contained information pertaining to certain BioPlus patients . . . The information subject to unauthorized access may have included your name, address, date of birth, Social Security number, medical record number, current/former member ID

[6] It is clear that the information exposed in the Data Breach was unencrypted: California law requires companies to notify California residents "whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person" due to a "breach of the security of the system[.]" Cal. Civ. Code § 1798.82(a)(1). Defendant notified the California Attorney General of the Data Breach on Dec. 10, 2021, evidencing that the exposed data was unencrypted.

[7] *See* Exhibit A (*Notice of Security Incident* archived by the California Attorney General).

[8] Exhibit B (Plaintiffs Grader's Redacted *Notice of Security Incident*) & Exhibit C (Plaintiffs Swanson's Redacted *Notice of Security Incident*).

number, claims information, diagnosis and/or prescription information.[9]

36. Defendant admits that an unauthorized party accessed electronic files that contained sensitive PII and PHI belonging to Plaintiffs and Class Members. Defendant also admits that the PII and PHI included names, dates of birth, Social Security numbers, and prescription information.

37. In response to the Data Breach, Defendant claims that they "have implemented, and will continue to adopt, additional safeguards and technical security measures to further protect and monitor our systems."[10] However, the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure a breach does not occur again have not been shared with the states' Attorneys General or Plaintiffs and Class Members, who retain a vested interest in ensuring that their information remains protected.

38. What's more, Defendant concedes that Plaintiffs and Class Members now face a present and immediate risk of identity theft because criminals had unhindered access to their PII and PHI for seventeen days before anyone stopped them. During this span of over two weeks, the unauthorized third parties took PII and PHI belonging to Plaintiffs and Class Members. Defendant warned Plaintiffs and Class Members in the Notice to "be vigilant for incidents of fraud or identity

[9] *Id.*
[10] Exhibit A.

theft by reviewing your account statements and free credit reports for any unauthorized activity."[11]

39. Plaintiffs' and Class Members' non-encrypted information may end up for sale on the dark web, or simply fall into the hands of companies that will use the detailed PII and PHI for targeted marketing without the approval of Plaintiffs and Class Members. Because of this Data Breach, unauthorized individuals can easily access the PII and PHI of Plaintiffs and Class Members.

40. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive PII and PHI, such as, at least, encrypting the information it was maintaining for Plaintiffs and Class Members, causing their PII and PHI to be exposed.

Defendant Acquired, Collected and Stored Plaintiffs' and Class Members' PII and PHI.

41. Defendant acquired, collected, and stored Plaintiffs' and Class Members' PII and PHI.

42. As a condition of their relationships with Plaintiffs and Class Members, Defendant required that Plaintiffs and Class Members entrust Defendant with highly sensitive, confidential PII and PHI.

43. By obtaining, collecting, and storing the PII and PHI of Plaintiffs and

[11] Exhibit B.

Class Members, Defendant assumed legal and equitable duties and knew or should have known that they were responsible for protecting the PII and PHI from disclosure.

44. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their PII and PHI and relied on Defendant to keep their PII and PHI confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

Securing PII and PHI and Preventing Breaches

45. Defendant could have prevented this Data Breach by properly securing and encrypting the PII and PHI of Plaintiffs and Class Members. Alternatively, Defendant could have destroyed the data that was no longer useful.

46. Defendant's negligence in safeguarding the PII and PHI of Plaintiffs and Class Members is exacerbated by the repeated warnings and alerts directed to businesses operating in the health industry to protect and secure sensitive data.

47. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the PII and PHI of Plaintiffs and Class Members from being compromised.

Defendant Failed to Comply with FTC Guidelines

37. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable

data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

38. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[12] The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[13]

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

---

[12] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Jan. 24, 2022).

[13] *Id.*

40. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

41. These FTC enforcement actions include actions against healthcare providers like Defendant. *See, e.g., In the Matter of Labmd, Inc., A Corp*, 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.").

42. Defendant failed to properly implement basic data security practices, such as encryption of data and actively monitoring for intrusions, which clearly did not happen here because it took seventeen days to discover the breach where an unauthorized party gained access to unencrypted PII and PHI.

43. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiffs' and Class Members' PII and PHI constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15

U.S.C. § 45.

44. Defendant was at all times fully aware of their obligation to protect the PII and PHI of Plaintiffs and Class Members. Defendant was also aware of the significant repercussions that would result from its failure to do so.

Defendant Failed to Comply with Industry Standards

45. Experts studying cyber security routinely identify businesses operating in the healthcare industry as being particularly vulnerable to cyberattacks because of the value of the PII and PHI that they collect and maintain.

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

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

follow these cybersecurity best practices, including failure to train staff.

48. Defendant failed to meet the minimum standards of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

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

Defendant Failed to Comply with HIPAA Standards of Conduct

61. HIPAA requires covered entities to protect against reasonably anticipated threats to the security of PHI. Covered entities must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical, and administrative components.[14]

62. Title II of HIPAA contains what are known as the Administrative

[14] HIPAA Journal, *What is Considered Protected Health Information Under HIPAA?*, *available at:* https://www.hipaajournal.com/what-is-considered-protected-health-information-under-hipaa/ (last visited Jan. 24, 2022).

Simplification provisions. 42 U.S.C. §§ 1301, *et seq*. These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling the type of PII and related data that Defendant left unguarded. The HHS has subsequently promulgated five rules under authority of the Administrative Simplification provisions of HIPAA.

63. The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, required Defendant to provide notice of the breach to each affected individual "without unreasonable delay and ***in no case later than 60 days following discovery of the breach***."[15]

64. Based on information and belief, Defendant's Data Breach resulted from a combination of insufficiencies that demonstrate that Defendant failed to comply with safeguards mandated by HIPAA regulations. Defendant's security failures include, but are not limited to, the following:

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

b. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only

[15] Breach Notification Rule, U.S. Dep't of Health & Human Services, *available at:* https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html (emphasis added) (last visited Jan. 24, 2022).

to those persons or software programs that have been granted access rights in violation of 45 C.F.R. §164.312(a)(1);

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

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

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

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

g. Failing to ensure compliance with HIPAA security standard rules by their workforce in violation of 45 C.F.R. §164.306(a)(4);

h. Impermissibly and improperly using and disclosing PHI that is and remains accessible to unauthorized persons in violation of 45 C.F.R. §164.502, *et seq.*;

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

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

Value of Personally Identifiable Information

65. It is well known that PII and PHI are invaluable commodities[16] and the frequent target of hackers. In 2019, a record 1,473 data breaches occurred, resulting in approximately 164,683,455 sensitive records being exposed, a 17% increase from 2018.[17] Of the 1,473 recorded data breaches, 525 of them, or 35.64%, were in the medical or healthcare industry.[18] The 525 reported breaches reported in 2019 exposed nearly 40 million sensitive records (39,378,157), compared to only 369 breaches that exposed just over 10 million sensitive records (10,632,600) in 2018.[19]

---

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

[17] https://www.idtheftcenter.org/wp-content/uploads/2020/01/01.28.2020_ITRC_2019-End-of-Year-Data-Breach-Report_FINAL_Highres-Appendix.pdf (last visited Jan. 24, 2022)

[18] *Id.*

[19] *Id* at p15.

66. Consumers place a high value not only on their PII, but also on the privacy of that data. This is because identity theft causes significant negative financial impact on victims as well as severe distress and other strong emotions and physical reactions.

67. Defendant was well aware that the PII and PHI they collect is highly sensitive and of significant value to those who would use it for wrongful purposes. PII and PHI is a valuable commodity to identity thieves. As the FTC recognizes, identity thieves can use this information to commit an array of crimes including identify theft, and medical and financial fraud.[20] Indeed, a robust "cyber black market" exists in which criminals openly post stolen PII and PHI on multiple underground Internet websites, commonly referred to as the dark web.

68. There is a market for Plaintiffs' and Class Members' PII and PHI, and the stolen PII and PHI has inherent value. Sensitive healthcare data can sell for as much as $363 per record according to the Infosec Institute.[21]

69. PHI is particularly valuable because criminals can use it to target victims with frauds and scams that take advantage of the victim's medical conditions or victim settlements. It can be used to create fake insurance claims, allowing for the

[20] Federal Trade Commission, *Warning Signs of Identity Theft, available at:* https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft (last visited Jan. 24, 2022).

[21] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), *available at:* https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last visited Jan. 24, 2022)

purchase and resale of medical equipment, or gain access to prescriptions for illegal use or resale.

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

71. Medical identity theft can result in inaccuracies in medical records and costly false claims. It can also have life-threatening consequences. If a victim's health information is mixed with other records, it can lead to misdiagnosis or mistreatment. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[22]

72. Similarly, the FBI Cyber Division, in an April 8, 2014 Private Industry Notification, advised:

[22] Michael Ollove, "The Rise of Medical Identity Theft in Healthcare," Kaiser Health News, Feb. 7, 2014, *available at:* https://khn.org/news/rise-of-indentity-theft/ (last visited Aug. 10, 2021).

> Cyber criminals are selling [medical] information on the black market at a rate of $50 for each partial EHR, compared to $1 for a stolen social security number or credit card number. EHR can then be used to file fraudulent insurance claims, obtain prescription medication, and advance identity theft. EHR theft is also more difficult to detect, taking almost twice as long as normal identity theft.[23]

73. The ramifications of Defendant's failure to keep their customers' PII and PHI secure are long lasting and severe. Once PII and PHI is stolen, fraudulent use of that information and damage to victims may continue for years. Fraudulent activity might not show up for six to 12 months or even longer.

74. Further, criminals often trade stolen PII and PHI on the "cyber black market" for years following a breach. Cybercriminals can post stolen PII and PHI on the internet, thereby making such information publicly available.

75. Defendant knew, or should have known, the importance of safeguarding the PII and PHI entrusted to it and of the foreseeable consequences if its data security systems were breached. This includes the significant costs that would be imposed on Defendant's clients, who are Plaintiffs and Class Members, because of a breach. Defendant failed, however, to take adequate cybersecurity measures to prevent the Data Breach.

---

[23] FBI Cyber Division, Private Industry Notification, "(U) Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain," Apr. 8, 2014, *available at:* http://www.illuminweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systems-cyber-intrusions.pdf (last visited Jan. 24, 2022).

CLASS ALLEGATIONS

76. Plaintiffs bring this nationwide class action on behalf of themselves and on behalf of all others similarly situated pursuant to Code of Civil Procedure § 382, Civil Code § 1781, and other applicable law.

77. The Nationwide Class that Plaintiffs seek to represent is defined as follows:

> **All individuals residing in the United States whose PII and PHI was exposed as a result of the data breach announced on December 12, 2021 (the "Nationwide Class").**

78. Excluded from the Classes are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has 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 their 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 their immediate family members.

79. Plaintiffs reserve the right to modify or amend the definition of the proposed classes before the Court determines whether certification is appropriate.

80. This action is brought and may be maintained as a class action because there is a well-defined community of interest among many persons who comprise a

readily ascertainable class. A well-defined community of interest exists to warrant class wide relief because Plaintiffs and all members of the Classes were subjected to the same wrongful practices by Defendant, entitling them to the same relief.

81. The Classes are so numerous that individual joinder of its members is impracticable.

82. Common questions of law and fact exist as to Class Members and predominate over any questions which affect only individual members of the Classes. These common questions include, but are not limited to:

a. Whether and to what extent Defendant had a duty to protect the PII and PHI of Plaintiffs and Class Members;

b. Whether Defendant had a duty not to disclose the PII and PHI of Plaintiffs and Class Members to unauthorized third parties;

c. Whether Defendant had a duty not to use the PII and PHI of Plaintiffs and Class Members for non-business purposes;

d. Whether Defendant failed to adequately safeguard the PII and PHI of Plaintiffs and Class Members;

e. Whether and when Defendant actually learned of the Data Breach;

f. Whether Defendant adequately, promptly, and accurately informed Plaintiffs and Class Members that their PII and PHI had been compromised;

g. Whether Defendant violated the law by failing to promptly notify Plaintiffs and Class Members that their PII and PHI had been compromised;

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

i. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII and PHI of Plaintiffs and Class Members;

k. Whether Plaintiffs and Class Members are entitled to actual, damages, and/or statutory damages as a result of Defendant's wrongful conduct;

l. Whether Plaintiffs and Class Members are entitled to restitution as a result of Defendant's wrongful conduct; and

m. Whether Plaintiffs and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

83. Plaintiffs are members of the Classes they seek to represent and their claims and injuries are typical of the claims and injuries of the other Class Members.

84. Plaintiffs will adequately and fairly protect the interests of other Class

Members. Plaintiffs have no interests adverse to the interests of absent Class Members. Plaintiffs are represented by legal counsel with substantial experience in class action litigation. The interests of Class Members will be fairly and adequately protected by Plaintiffs and their counsel.

85. Defendant has acted or refused to act on grounds that apply generally to the Class Members, so that final injunctive relief or corresponding declaratory relief is appropriate respecting the Class as a whole.

86. A class action is superior to other available means for fair and efficient adjudication of the claims of the Class and would be beneficial for the parties and the court. Class action treatment will allow a large number of similarly situated persons to prosecute their common claims in a single forum, simultaneously, efficiently, and without the unnecessary duplication of effort and expense that numerous individual actions would require. The amounts owed to the many individual Class Members are likely to be relatively small, and the burden and expense of individual litigation would make it difficult or impossible for individual members of the class to seek and obtain relief. A class action will serve an important public interest by permitting such individuals to effectively pursue recovery of the sums owed to them. Further, class litigation prevents the potential for inconsistent or contradictory judgments raised by individual litigation. Plaintiffs is unaware of any difficulties that is likely to be encountered in the management of this action that

would preclude its maintenance as a class action.

COUNT I
Negligence
(On Behalf of Plaintiffs and the Nationwide Class)

87. Plaintiffs and the Classes re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 86.

88. Plaintiffs and Class Members provided and entrusted Defendant with certain PII and PHI, including but not limited to their Social Security numbers, names, addresses, dates of birth, medical record numbers, current/former member ID numbers, claims information, and diagnosis and/or prescription information.

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

90. Defendant has full knowledge of the sensitivity of the PII and PHI and the types of harm that Plaintiffs and Class Members could and would suffer if the PII and PHI were wrongfully disclosed.

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

92. Defendant had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendant's security protocols to ensure that the PII and PHI of Plaintiffs and Class Members in Defendant's possession was adequately secured and protected.

93. Defendant also had a duty to exercise appropriate clearinghouse practices to remove PII and PHI it was no longer required to retain pursuant to regulations.

94. Defendant also had a duty to have procedures in place to detect and prevent the improper access and misuse of the PII and PHI of Plaintiffs and Class Members.

95. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiffs and Class Members, which is recognized by laws and regulations including but not limited to HIPAA, as well as the common law. That a special relationship arose because Plaintiffs and Class Members entrusted Defendant with their confidential PII and PHI, a necessary part of their relationships with Defendant.

96. Defendant's duty to use reasonable security measures under HIPAA required Defendant to "reasonably safeguard" confidential data from "any

intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c).

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

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

99. Defendant is subject to an "independent duty," untethered to any contract between Defendant and Plaintiffs or Class Members.

100. A breach of security, unauthorized access, and resulting injury to Plaintiffs and Class Members was reasonably foreseeable, particularly in light of Defendant's inadequate security practices, including sharing and/or storing the PII and PHI of Plaintiffs and Class Members on its systems.

101. Plaintiffs and Class Members were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the PII and PHI of Plaintiffs and Class Members, the critical importance of providing adequate security

of that PII and PHI, and the necessity for encrypting PII and PHI stored on Defendant's systems.

102. Defendant's own conduct created a foreseeable risk of harm to Plaintiffs and Class Members. Defendant's misconduct included, but was not limited to, their failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included their decisions not to comply with industry standards for the safekeeping of the PII and PHI of Plaintiffs and Class Members, including basic encryption techniques freely available to Defendant.

103. Plaintiffs and Class Members had no ability to protect their PII and PHI that was in, and possibly remains in, Defendant's possession.

104. Defendant was in a position to protect against the harm suffered by Plaintiffs and Class Members as a result of the Data Breach.

105. Defendant had and continues to have a duty to adequately disclose that the PII and PHI of Plaintiffs and Class Members within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiffs and Class Members to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties.

106. Defendant has a duty to employ proper procedures to prevent the unauthorized dissemination of the PII and PHI of Plaintiffs and Class Members.

107. Defendant admitted that the PII and PHI of Plaintiffs and Class Members was wrongfully accessed by unauthorized actors as a result of the Data Breach.

108. Defendant, through their actions and/or omissions, unlawfully breached their duties to Plaintiffs and Class Members by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the PII and PHI of Plaintiffs and Class Members during the time the PII and PHI were within Defendant's possession or control.

109. Defendant improperly and inadequately safeguarded the PII and PHI of Plaintiffs and Class Members in deviation of standard industry rules, regulations, and practices at the time of the Data Breach, including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2 of the NIST Cybersecurity Framework Version 1.1.

110. Defendant failed to heed industry warnings and alerts to provide adequate safeguards to protect the PII and PHI of Plaintiffs and Class Members in the face of increased risk of theft.

111. Defendant, through their actions and/or omissions, unlawfully breached their duty to Plaintiffs and Class Members by failing to have appropriate procedures in place to detect and prevent dissemination of their PII and PHI, which is evidenced

by the fact that it took Defendant over two weeks to even discover the Data Breach.

112. Defendant breached their duty to exercise appropriate clearinghouse practices by failing to remove PII and PHI that was no longer required to retain pursuant to regulations.

113. Defendant, through its actions and/or omissions, unlawfully breached their duty to adequately and timely disclose to Plaintiffs and Class Members the existence and scope of the Data Breach.

114. But for Defendant's wrongful and negligent breach of duties owed to Plaintiffs and Class Members, the PII and PHI of Plaintiffs and Class Members would not have been compromised.

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

116. Additionally, Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable

measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

117. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiffs and Class Members.

118. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se*.

119. Plaintiffs and Class Members are within the class of persons that the FTC Act was intended to protect.

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

121. Defendant's misconduct also included their decision not to comply with HIPAA for the reporting, safekeeping and encrypted authorized disclosure of the PHI of Plaintiffs and Class Members.

122. HIPAA privacy laws were enacted with the objective of protecting the confidentiality of patients' healthcare information and set forth the conditions under which such information can be used, and to whom it can be disclosed. HIPAA privacy laws not only apply to healthcare providers and the organizations they work for, but to any entity that may have access to healthcare information about a patient that—if it were to fall into the wrong hands—could present a risk of harm to the patient's finances or reputation.

123. Plaintiffs and Class Members are within the class of persons that HIPAA privacy laws were intended to protect.

124. The harm that occurred as a result of the Data Breach is the type of harm HIPAA privacy laws were intended to guard against.

125. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiffs 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 PII and PHI is used; (iii) the compromise, publication, and/or theft of their PII and PHI; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII and PHI; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent

researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII and PHI, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of Plaintiffs and Class Members; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

126. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiffs 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.

127. Additionally, as a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiffs and Class Members have suffered and will suffer the continued risks of exposure of their PII and PHI, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fail to undertake appropriate and adequate measures to protect the PII in its continued possession.

COUNT II
Breach of Implied Contract
(On Behalf of Plaintiffs and the Nationwide Class)

128. Plaintiffs and the Classes re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 86.

129. Through their course of conduct, Defendant, Plaintiffs, and Class Members entered into implied contracts for Defendant to implement data security adequate to safeguard and protect the privacy of their PII and PHI.

130. Defendant required Plaintiffs and Class Members to provide and entrust their PII and PHI, including Social Security numbers, names, birthdates, and medical information, as a condition of receiving services from Defendant.

131. Defendant solicited and invited Plaintiffs and Class Members to provide their PII and PHI as part of their regular business practices. Plaintiffs and Class Members accepted Defendant's offers and provided their PII and PHI to Defendant.

132. As a condition of being customers of Defendant, Plaintiffs and Class Members provided and entrusted their PII and PHI to Defendant. In so doing, Plaintiffs and Class Members entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such non-public information, to keep such information secure and confidential, and to timely and accurately notify

Plaintiffs and Class Members if their data had been breached and compromised or stolen.

133. A meeting of the minds occurred when Plaintiffs and Class Members agreed to, and did, provide their PII and PHI to Defendant, in exchange for, amongst other things, the protection of their Private Information.

134. Plaintiffs and Class Members fully performed their obligations under the implied contracts with Defendant.

135. Defendant breached the implied contracts it made with Plaintiffs and Class Members by failing to safeguard and protect their PII and PHI by failing to provide timely and accurate notice to them that their PII and PHI was compromised as a result of the Data Breach.

136. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiffs and Class Members have suffered (and will continue to suffer) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and

credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

137. As a direct and proximate result of Defendant's breach of the implied contracts, Plaintiffs and Class Members sustained damages as alleged herein.

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

COUNT III
Declaratory Judgment
(On Behalf of Plaintiffs and the Nationwide Class)

139. Plaintiffs and the Classes re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 138.

140. Under the Declaratory Judgment Act, 28 U.S.C. § 2201, et seq., the Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this complaint.

141. An actual controversy has arisen in the wake of the Data Breach regarding Defendant's present and prospective common law and other duties to reasonably safeguard its users' PII, and whether Defendant is currently maintaining data security measures adequate to protect Plaintiff and Class Members from further

data breaches that compromise their PII and PHI. Plaintiff and Class Members remain at imminent risk that further compromises of their PII and PHI will occur in the future. This is true even if they (or their healthcare providers) are not actively using Defendant's products or services.

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

a. Defendant continues to owe a legal duty to secure users' PII and PHI and to timely notify consumers of a data breach under the common law and Section 5 of the FTC Act;

b. Defendant continues to breach this legal duty by failing to employ reasonable measures to secure Plaintiffs' and Class Members' PII and PHI.

143. The Court also should issue corresponding prospective injunctive relief pursuant to 28 U.S.C. §2202, requiring Defendant to employ adequate security practices consistent with law and industry standards to protect its users' PII and PHI.

144. If an injunction is not issued, Plaintiffs and Class Members will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach of Defendant's systems. The risk of another such breach is real, immediate, and substantial. If another breach occurs, Plaintiffs and Class Members will not have an adequate remedy at law because many of the resulting injuries are not readily

quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

145. The hardship of Plaintiffs and Class Members if an injunction does not issue exceeds the hardship to Defendant if an injunction is issued. Among other things, if another data breach occurs, Plaintiffs and Class Members will likely be subjected to fraud, identity theft, and other harms described herein. On the other hand, the cost to Defendant of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendant has pre-existing legal obligation to employ such measures.

146. Issuance of the request injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach of Defendant's systems, thus eliminating additional injuries that would result to Plaintiffs, Class Members, and the millions of other customers of Defendant whose PII and PHI would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and Class Members, request judgment against Defendant and that the Court grant the following:

A. For an Order certifying the Nationwide Class and the California Class, and appointing Plaintiffs and their Counsel to represent each such Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII and PHI of Plaintiffs and Class Members;

C. For injunctive relief requested by Plaintiffs, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members, including but not limited to an order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

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

iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiffs and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members;

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the

confidentiality and integrity of the PII and PHI of Plaintiffs and Class Members;

v. prohibiting Defendant from maintaining the PII and PHI of Plaintiffs and Class Members on a cloud-based database;

vi. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

ix. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

x. requiring Defendant to conduct regular database scanning and

securing checks;

xi. requiring Defendant 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 personal identifying information, as well as protecting the personal identifying information of Plaintiffs and Class Members;

xii. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

xiv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to

appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Defendant 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;

xvi. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

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

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

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demands that this matter be tried before a jury.

Date: January 26, 2022

Respectfully Submitted,

/s/ Katherine Earle Yanes

Katherine Earle Yanes (FB# 159727)
KYNES, MARKMAN & FELMAN, P.A.
P.O. Box 3396
Tampa, FL 33601-3396
Telephone: (813) 229-1118
Facsimile: (813) 221-6750
Kyanes@kmf-law.com
Local Counsel for Plaintiffs and the Putative Class

Gary Mason*
David K. Lietz*
E-mail: dlietz@masonllip.com
MASON LIETZ & KLINGER LLP
5301 Wisconsin Avenue, NW. Suite 305
Washington, DC 20016
Tel: (202) 429-2290

Gary M. Klinger*
E-mail: gklinger@masonllip.com
MASON LIETZ & KLINGER LLP
227 West Monroe Street, Suite 2100
Chicago, IL 60606
Tel: (202) 429-2290

M. Anderson Berry*
Gregory Haroutunian*
CLAYEO C. ARNOLD,
A PROFESSIONAL LAW CORP.
865 Howe Avenue
Sacramento, CA 95825
Telephone: (916) 777-7777
Facsimile: (916) 924-1829
aberry@justice4you.com

Attorneys for Plaintiffs and the Putative Class

* *Pro Hac Vice* Forthcoming.