Exhibit A-1

UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF FLORIDA
ORLANDO DIVISION

BONNIE GILBERT, on behalf of herself and all others similarly situated, **Plaintiff,** **v.** **BIOPLUS SPECIALTY PHARMACY SERVICES, LLC,** **Defendant.**	Case No. **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Bonnie Gilbert ("Plaintiff"), by and through her attorneys, upon personal knowledge as to herself and her own acts and experiences, and upon information and belief as to all other matters, alleges as follows:

NATURE OF THE ACTION

1. Defendant BioPlus Specialty Pharmacy Services, LLC ("BioPlus" or "Defendant") is a national specialty pharmacy that provides a complete range of specialty pharmacy services for patients with cancer, infusion, multiple sclerosis, hepatitis C, and other complex chronic conditions.

2. This action arises out of a recent data breach (the "Data Breach") involving information on Defendant's network, including the personally identifiable information ("PII") of its patients, such as names, dates of birth, addresses, and Social Security numbers, as well as protected health information ("PHI"), such as medical record numbers, current/former health plan member ID numbers, claims information, prescription medication information, and diagnoses

(PHI and PII are referred to collectively as "Sensitive Information").

3. In total, the Data Breach compromised the Sensitive Information of approximately 350,000 current and former BioPlus patients ("Class Members").

4. BioPlus is responsible for allowing this Data Breach through its failure to implement and maintain reasonable data security safeguards, failure to exercise reasonable care in the hiring and supervision of its employees and agents, and failure to comply with industry-standard data security practices as well as federal and state laws and regulations governing data security and privacy, including security of PII and PHI.

5. Despite its role in managing so much sensitive and personal PII and PHI, Defendant failed to recognize and detect unauthorized third parties accessing its network, and failed to recognize the substantial amounts of data that had been compromised. Had Defendant properly maintained and monitored its information technology infrastructure, it would have discovered the invasion sooner – and/or prevented it altogether.

6. Defendant had numerous statutory, regulatory, and common law duties to Plaintiff and the Class Members to keep their PII, including PHI, confidential, safe, secure, and protected from unauthorized disclosure or access, including duties under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). Plaintiff and Class Members rely upon Defendant to maintain the security and privacy of the Sensitive Information entrusted to it; when providing their Sensitive Information, they reasonably expected and understood that Defendant would ensure that it would comply with the obligation to keep Plaintiff's Sensitive Information secure and safe from unauthorized access.

7. In this era of frequent data security attacks and data breaches, particularly in the healthcare industry, Defendant's failures leading to the Data Breach are particularly egregious.

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

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

10. Plaintiff and Class Members 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.

11. As a result of Defendant's failures to protect the PII and PHI of Plaintiff and Class Members, their PII and PHI were accessed and downloaded by malicious cyber criminals, who targeted that information through their wrongdoing. As a direct and proximate result, Plaintiff and the Class Members are now at a significant present and future risk of identity theft, financial fraud, and/or other identity-theft or fraud, imminently and for years to come.

12. Plaintiff and Class Members have now lost the economic value of their PII and PHI. Indeed, there is both a healthy black market and a legitimate market for that PII and PHI. Just as Plaintiff's and Class Members' PII and PHI were stolen, *inter alia*, because of its inherent value in the black market, the inherent value of Plaintiff and the Class Members' PII and PHI in the legitimate market is now significantly and materially decreased.

13. Plaintiff and Class Members have suffered numerous actual and imminent injuries as a direct result of the Data Breach, including: (a) theft of their PII and PHI; (b) costs associated with the detection and prevention of identity theft; (c) costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the

consequences of the Data Breach; (d) invasion of privacy; (e) the emotional distress, stress, nuisance, and annoyance of responding to, and resulting from, the Data Breach; (f) the actual and/or imminent injury arising from actual and/or potential fraud and identity theft posed by their personal data being placed in the hands of the ill-intentioned hackers and/or criminals; (g) damages to and diminution in value of their personal data entrusted to Defendant with the mutual understanding that Defendant would safeguard Plaintiff's and Class Members' PII and PHI against theft and not allow access and misuse of their personal data by others; and (h) the continued risk to their PII and PHI, which remains in the possession of Defendant, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' PII and PHI.

14. Plaintiff seeks to remedy these harms, and to prevent their future occurrence, on behalf of herself and all similarly situated persons whose PII and PHI were compromised as a result of the Data Breach.

15. Accordingly, Plaintiff, on behalf of herself and other Class Members, asserts claims for negligence, negligence *per se*, and declaratory judgment. Plaintiff seeks injunctive relief, declaratory relief, monetary damages, and all other relief as authorized in equity or by law.

THE PARTIES

Plaintiff Bonnie Gilbert

16. Plaintiff Bonnie Gilbert is a natural person and a resident of Georgia.

17. Plaintiff 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.

18. Recognizing the substantial risk Plaintiff faces, Defendant provided Plaintiff a one-year subscription to a credit monitoring service. However, Plaintiff was forced to spend time signing up for this service. Moreover, Plaintiff will be forced to incur costs to maintain this service after her subscription expires in one year.

19. Plaintiff was forced to spend significant time speaking with her local pharmacy to place a fraud alert so that moving forward, no one can pick up Plaintiff's prescriptions on her behalf unless Plaintiff has calls ahead and gives preauthorization. Plaintiff will be forced to spend significant time in the future providing preauthorization for others to pick up her medication.

20. Since learning of the Data Breach, Plaintiff has spent time every day reviewing her bank statements and credit cards. Plaintiff has also spent significant time speaking with her bank regarding her concerns about the Data Breach, in part because she spent approximately $90 ordering new checks before learning of the Data Breach, and if she changes her checking account information, she will lose the $90 that she just spent to obtain the new checks.

21. The Data Breach has caused Plaintiff to suffer significant fear, anxiety, and stress. Plaintiff 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.

22. Plaintiff plans on taking additional time-consuming, yet necessary, steps to help mitigate the harm caused by the Data Breach, such as implementing credit freezes.

Defendant BioPlus

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

24. BioPlus advertises itself as its patients' "24/7 partner in health." It helps provides 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."[1]

JURISDICTION & VENUE

25. 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 interest and costs. Moreover, Plaintiff Gilbert as a resident of Georgia and Defendant are citizens of different states. According one of its recent business filing with the Florida Secretary of State, BioPlus's principal place of business is in this District and it has manager members who are residents of the State of Florida and an authorized member named BioPlus Parent, LLC that is a resident of the Rhode Island with an address of 50 Kennedy Plaza, 12th Floor, Providence, RI 02903.[2] Furthermore, members of the class are located in various other states, such as California and Montana, according to the data breach notifications BioPlus issued to those states' Attorney Generals.[3] Accordingly, minimal diversity under CAFA exists given that the members of BioPlus as an LLC are minimally diverse from members of the Class.

26. 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.

27. Venue is proper in this District under 28 U.S.C. §§1391(a)(2), 1391(b)(2), and

[1] https://bioplusrx.com/patients/personalized-support/ (last visited December 23, 2021).

[2] https://search.sunbiz.org/Inquiry/CorporationSearch/GetDocument?aggregateId=flal-l20000120596-5c9eb297-ea42-4079-afba-d91a65cb2e1b&transactionId=l20000120596-d098315b-c625-4630-b486-b6ff162c41b0&formatType=PDF (last visited on December 27, 2021).

[3] https://oag.ca.gov/ecrime/databreach/reports/sb24-548450 (reporting to the California Attorney General is required for data breaches affected 500 or more California residents) (last visited on December 27, 2021); https://dojmt.gov/consumer/databreach/ (noting that at least 534 Montana residents were impacted by the BioPlus data breach) (last visited on December 27, 2021).

1391(c)(2) as a substantial part of the events giving rise to the claims emanated from activities within this District, and Defendant conducts substantial business in this District.

FACTUAL ALLEGATIONS

The Data Breach

28. On or about November 11, 2021, BioPlus identified suspicious activity in its IT network. BioPlus later determined that an unauthorized party gained access to its IT network between October 25, 2021 and November 11, 2021. During that time, the unauthorized party accessed files containing the Sensitive Information of BioPlus's patients.

29. BioPlus did not begin notifying its patients that their Sensitive Information had been compromised until it began mailing notification letters, such as the one received by Plaintiff, on or about December 10, 2021.

30. The letters received by Plaintiff and Class Members indicate that the following Sensitive Information was exposed in the breach: patient names, dates of birth, addresses, medical record numbers, current/former health plan member ID numbers, claims information, diagnoses, and/or prescription information. BioPlus has disclosed that certain patients, such as Plaintiff, also had their Social Security numbers exposed in the breach.

31. The notification letters provided to Plaintiff and Class Members recommend several time-consuming steps that victims of the Data Breach can take to try to mitigate the risk of future fraud and identity theft, such as fraud alerts and credit freezes.

32. Patients whose Social Security numbers were determined to be exposed in the Data Breach, such as Plaintiff, were offered a one-year subscription to Experian credit monitoring and identity protection services. BioPlus has not offered to extend this credit monitoring longer than one year Plaintiff and Class Members facing a substantial risk of fraud and identity theft both now

and for years to come.

33. But for Defendant's failure to take reasonable steps to secure Plaintiff's and Class Members' Sensitive Information and to exercise reasonable care in the hiring and/or supervision of its employees, malicious actors would not have been able to gain access to Defendant's network.

34. It is common sense that the criminal(s) that breached Defendant's systems and acquired the victims' PII and PHI did so for the purpose of using that data to commit fraud, theft, and other crimes, or for the purpose of the selling or providing the PII and PHI to other individuals intending to commit fraud, theft, and other crimes. Given that this is the reason such PII and PHI are sought by criminals, it is similarly common sense that Plaintiff and the Class Members have already suffered injury and face a substantial risk for imminent and certainly impending future injury.

35. Defendant acknowledged the risk faced by victims of the Data Breach. For example, Defendant has offered to provide Plaintiff with a one-year membership to credit monitoring services. It is common sense that Defendant would not pay for such services if it did not believe Plaintiff and Class Members faced a substantial risk of harm from the exposure of their Sensitive Information in the Data Breach.

36. According to the Federal Trade Commission ("FTC"), identity theft wreaks havoc on consumers' finances, credit history, and reputation and can take time, money, and patience to resolve.[4] Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank and finance fraud.[5]

---

[4] *See Taking Charge, What to Do If Your Identity is Stolen*, FTC, 3 (2012), http://www.consumer.ftc.gov/articles/pdf-0009-taking-charge.pdf (last visited April 20, 2021). https://www.consumer.ftc.gov/articles/pdf-0009_identitytheft_a_recovery_plan.pdf.

[5] *Id.* The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 CFR § 603.2. 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

37. The physical, emotional, and social toll suffered (in addition to the financial toll) by identity theft victims cannot be understated.[6] "A 2016 Identity Theft Resource Center survey of identity theft victims sheds light on the prevalence of this emotional suffering caused by identity theft: 74 percent of respondents reported feeling stressed, 69 percent reported feelings of fear related to personal financial safety, 60 percent reported anxiety, 42 percent reported fearing for the financial security of family members, and 8 percent reported feeling suicidal."[7]

38. More recently, the FTC released an updated publication on protecting PII for businesses, which includes instructions on protecting PII, properly disposing of PII, understanding network vulnerabilities, implementing policies to correct security problems, using intrusion detection programs, monitoring data traffic, and having in place a response plan.

39. The FTC has brought enforcement actions against businesses for failing to protect customers' PII. The FTC has done this by treating a failure to employ reasonable measures to protect against unauthorized access to PII as a violation of the FTC Act, 15 U.S.C. §45.

40. Identity thieves may commit various types of crimes such as, *inter alia*, immigration fraud, obtaining a driver's license or identification card in the victim's name but with another's picture, fraudulently obtaining medical services, and/or using the victim's information to obtain a fraudulent tax refund.

41. The United States government and privacy experts acknowledge that it may take years for identity theft to come to light and be detected. Moreover, identify thieves may wait years before using the stolen data.

---

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." *Id.*

[6] *Id.*

[7] *Id.*

42. Because the information Defendant allowed to be compromised and taken is of such a durable and permanent quality (*i.e.*, names, Social Security Numbers, dates of birth, and PHI), the harms to Plaintiff and the Class will continue and increase, and Plaintiff and the Class will continue to be at substantial risk for further imminent and future harm.

Defendant Knew It Was and Continues to Be a Prime Target for Cyberattacks.

43. Defendant is fully aware of how sensitive the PII and PHI it stores and maintains is. It is also aware of how much PII and PHI it collects, uses, and maintains from Plaintiff and Class Members.

44. Defendant knew or should have known that it was an ideal target for hackers and those with nefarious purposes related to sensitive personal and health data. It processed and saved multiple types, and many levels, of PII and PHI through its computer data and storage systems.

45. By requiring the production of, collecting, obtaining, using, and deriving benefits from Plaintiff's and the Class Members' PII and PHI, Defendant assumed certain legal and equitable duties, and it knew or should have known that it was responsible for the diligent protection of that PII and PHI it collected and stored.

46. As a large and highly successful company, Defendant had the resources to invest in the necessary data security and protection measures. Yet, Defendant failed to exercise reasonable care in the hiring and/or supervision of its employees and agents and failed to undertake adequate analyses and testing of its own systems, adequate personnel training, and other data security measures to avoid the failures that resulted in the Data Breach.

47. The seriousness with which Defendant should have taken its data security is shown by the number of data breaches perpetrated in the healthcare industry over the past few years.

48. Over 41 million patient records were breached in 2019, with a single hacking

incident affecting close to 21 million records.[8] Healthcare breaches in 2019 almost tripled those the healthcare industry experienced in 2018, when 15 million patient records were affected by data breach incidents, according to a report from Protenus and DataBreaches.net.[9]

49. Protenus, a healthcare compliance analytics firm, analyzed data breach incidents disclosed to the U.S. Department of Health and Human Services or the media during 2019, finding that there has been an alarming increase in the number of data breaches of patient privacy since 2016, when there were 450 security incidents involving patient data. [10] In 2019 that number jumped to 572 incidents, which is likely an underestimate, as two of the incidents for which there were no data affected 500 dental practices and clinics and could affect significant volumes of patient records. There continues to be on average at least one health data breach every day.[11]

50. One recent report found that in 2020, healthcare was one of the industries most affected by tracked ransomware incidents.[12]

PII and PHI Are Very Valuable

51. At an FTC public workshop in 2001, then-Commissioner Orson Swindle described the value of a consumer's personal information as follows:

> The use of third party information from public records, information aggregators and even competitors for marketing has become a major facilitator of our retail economy. Even [Federal Reserve] Chairman [Alan] Greenspan suggested here some time ago that it's something on the order of the life blood, the free flow of

[8] Heather Landi, *Number of patient records breached nearly triples in 2019*, FIERCE HEATLHCARE (Feb. 20, 2020), https://www.fiercehealthcare.com/tech/number-patient-records-breached-2019-almost-tripled-from-2018-as-healthcare-faces-new-threats#:~:text=Over%2041%20million%20patient%20records,close%20to%2021%20million%20records (last visited December 23, 2021).
[9] *Id.*
[10] *Id.*
[11] *Id.*
[12] Kat Jerich, *Healthcare hackers demanded an average ransom of $4.6 last year, says BakerHostetler*, HEALTHCARE IT NEWS (May 4, 2021), https://www.healthcareitnews.com/news/healthcare-hackers-demanded-average-ransom-46m-last-year-says-bakerhostetler (last visited December 23, 2021).

information.[13]

52. Consumers rightfully place a high value not only on their PII and PHI, but also on the privacy of that data. Researchers have already begun to shed light on how much consumers value their data privacy – and the amount is considerable. Notably, one study on website privacy determined that U.S. consumers valued the restriction of improper access to their personal information – the very injury at issue here – between $11.33 and $16.58 per website. The study also determined that "[a]mong U.S. subjects, protection against errors, improper access, and secondary use of personal information is worth US$30.49 – 44.62."[14] This study was done in 2002, almost twenty years ago. The sea-change in how pervasive the Internet is in everyday lives since then indicates that these values—when associated with the loss of PII and PHI to bad actors—would be exponentially higher today.

The PII and PHI at Issue Here is Particularly Valuable to Hackers

53. Businesses that store personal information are likely to be targeted by cyber criminals. Credit card and bank account numbers are tempting targets for hackers, but credit and debit cards can be cancelled, quickly mitigating the hackers' ability to cause further harm. Instead, PHI and types of PII that cannot be easily changed (such as dates of birth and Social Security Numbers) are the most valuable to hackers.[15]

54. The unauthorized disclosure of Social Security numbers can be particularly

---

[13] *The Information Marketplace: Merging and Exchanging Consumer Data*, FTC (Mar. 13, 2001), *transcript available* at http://www.ftc.gov/news-events/events-calendar/2001/03/information-marketplace-merging-exchanging-consumer-data (last visited December 23, 2021).

[14] Il-Horn Hann, Kai-Lung Hui, *et al*, *The Value of Online Information Privacy: Evidence from the USA and Singapore*, at 17. Marshall Sch. Bus., Univ. So. Cal. (Oct. 2002), https://www.comp.nus.edu.sg/~ipng/research/privacy.pdf (last visited December 23, 2021).

[15] *Calculating the Value of a Data Breach – What Are the Most Valuable Files to a Hacker?* Donnellon McCarthy Enters., https://www.dme.us.com/2020/07/21/calculating-the-value-of-a-data-breach-what-are-the-most-valuable-files-to-a-hacker/ (last visited December 23, 2021).

damaging, because Social Security numbers cannot easily be replaced. In order to obtain a new Social Security number a person must prove, among other things, that he or she continues to be disadvantaged by the misuse. Thus, no new Social Security number can be obtained until the damage has been done.

55. Furthermore, as the Social Security Administration ("SSA") warns:

> Keep in mind that a new number probably will not solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) likely will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number will not guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same.
>
> If you receive a new Social Security Number, you should not be able to use the old number anymore.
>
> For some victims of identity theft, a new number actually creates new problems. If the old credit information is not associated with your new number, the absence of any credit history under the new number may make more difficult for you to get credit.[16]

56. Criminals can, for example, use Social Security numbers to create false bank accounts or file fraudulent tax returns.[17] Victims of the Data Breach will spend, and already have spent, time contacting various agencies, such as the Internal Revenue Service and the Social Security Administration. They also now face a real and imminent substantial risk of identity theft and other problems associated with the disclosure of their Social Security number and will need to monitor their credit and tax filings for an indefinite duration.

57. PHI is just as, if not more, valuable than Social Security Numbers. According to a

---

[16] SSA, *Identity Theft and Your Social Security Number*, SSA Publication No. 05-10064 (Dec. 2013), http://www.ssa.gov/pubs/EN-05-10064.pdf (last visited December 23, 2021).

[17] When fraudulent tax returns are filed, the requirements for a legitimate taxpayer to file their tax returns with the IRS increase, including the necessity to obtain and utilize unique PIN numbers just to be able to file a tax return.

report by the Federal Bureau of Investigation's ("FBI") Cyber Division, healthcare records can be sold by criminals for 50 times the price of stolen Social Security numbers or credit card numbers.[18] A file containing private health insurance information can be bought for between $1,200 and $1,300 ***each*** on the black market.[19]

58. Similarly, the most recent edition of the annual Baker Hostetler Data Security Incident Response Report found that in 2020, hackers in ransomware attacks made an average initial ransomware demand of $4,583,090 after obtaining PHI. In 2020, final payouts to hackers committing ransomware attacks involving PHI averaged $910,335.[20]

59. Companies recognize that PII and PHI are valuable assets. Indeed, PII and PHI are valuable commodities. A "cyber black-market" exists in which criminals openly post stolen PII and PHI on a number of Internet websites. Plaintiff's and Class Members' compromised PII has a high value on both legitimate and black markets.

60. Some companies recognize PII, and especially PHI, as a close equivalent to personal property. Software has been created by companies to value a person's identity on the black market. The commoditization of this information is thus felt by consumers as theft of personal property in addition to an invasion of privacy.

61. Moreover, compromised health information can lead to falsified information in medical records and fraud that can persist for years as it "is also more difficult to detect, taking

---

[18] *FBI Cyber Division Bulletin: Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain*, FBI (April 8, 2014), https://publicintelligence.net/fbi-health-care-cyber-intrusions/ (last visited December 23, 2021).

[19] Elizabeth Clarke, *Hackers Sell Health Insurance Credentials, Bank Accounts, SSNs and Counterfeit Documents*, SecureWorks (July 15, 2013), https://www.secureworks.com/blog/general-hackers-sell-health-insurance-credentials-bank-accounts-ssns-and-counterfeit-documents (last visited December 23, 2021).

[20] Jerich, *supra* n.10.

twice as long as normal identity theft."[21]

62. Because the information Defendant allowed to be compromised and taken is of such a durable and permanent quality, the harms to Plaintiff and the Class will continue and increase, and Plaintiff and Class Members will continue to be at substantial risk for further imminent and future harm.

Defendant's Post-Breach Activity Was (and Remains) Inadequate

63. Immediate notice of a security breach is essential to protect victims such as Plaintiff and Class Members. Defendant failed to provide such immediate notice, thus further exacerbating the harm to Plaintiff and Class Members resulting from the Data Breach.

64. Such failure to protect Plaintiff's and Class Members' PII and PHI, and timely notify them of the Data Breach, has significant ramifications. The information stolen allows criminals to commit theft, identity theft, and other types of fraud. Moreover, because the data points stolen are persistent—for example, names, dates of birth, Social Security numbers, and prescription medication data—as opposed to transitory, criminals who access, stole, or purchase the PII and PHI belonging to Plaintiff and the Class Members, do not need to use the information to commit fraud immediately. The PII and PHI can be used or sold for use years later, and often is.

65. Plaintiff and Class Members are now at a significant risk of imminent and future fraud, misuse of their PII and PHI, and identity theft for many years in the future as a result of the Defendant's actions and the Data Breach. The theft of their PHI is particularly impactful, as many banks or credit card providers have substantial fraud detection systems with quick freeze or cancellation programs in place, whereas the breadth and usability of PHI allows criminals to get

[21] *See* FBI, *supra* n.16.

away with misuse for years before healthcare-related fraud is spotted.

66. Plaintiff and Class Members have suffered real and tangible losses, including but not limited to the loss in the inherent value of their PII and PHI, the loss of their time as they have had to spend additional time monitoring accounts and activity, and additional economic loss to mitigate the costs of injuries realized as a result of discovery in this case, but until recently, kept silent by Defendant.

67. Despite Defendant's egregious failure to protect Plaintiff's PII and PHI, it has only offered to provide them with trivial compensation or remedy, such as one-year of credit monitoring or identity protection services.

CLASS ACTION ALLEGATIONS

68. Pursuant to the provisions of Fed. R. Civ. P. 23(a), 23(b)(1), 23(b)(2), 23(b)(3), and 23(c)(4), Plaintiff seeks to bring this class action on behalf of herself and a nationwide class (the "Class") defined as:

> **All persons who reside in the United States whose PII and PHI was compromised by the Data Breach.**

69. Excluded from the Class are Defendant; officers, directors, and employees of Defendant; any entity in which Defendant has a controlling interest, is a parent or subsidiary, or which is controlled by Defendant; and the affiliates, legal representatives, attorneys, heirs, predecessors, successors, and assigns of Defendant. Also excluded are the Judges and Court personnel in this case and any members of their immediate families.

70. Plaintiff reserves the right to modify and/or amend the Class definition, including but not limited to creating additional subclasses, as necessary.

71. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of the claims on a class-wide basis using the same evidence as

would be used to prove those elements in individual actions alleging the same claims.

72. All Class Members are readily ascertainable in that Defendant has access to addresses and other contact information for all Class Members, which can be used for providing notice to Class Members.

73. ***Numerosity***. The Class is so numerous that joinder of all members is impracticable. The Class includes roughly 350,000 individuals whose personal data was compromised by the Data Breach.

74. ***Commonality and Predominance***. There are numerous questions of law and fact common to Plaintiff and the Class that predominate over any questions that may affect only individual Class Members, including the following:

- whether Defendant engaged in the wrongful conduct alleged in this Complaint;
- whether Defendant's conduct was unlawful;
- whether Defendant failed to implement and maintain reasonable systems and security procedures and practices to protect customers' personal data;
- Whether Defendant failed to exercise reasonable care in the hiring of its employees and agents;
- Whether Defendant failed to exercise reasonable care in the supervision of its employees and agents;
- whether Defendant unreasonably delayed in notifying affected customers of the Data Breach;
- whether Defendant owed a duty to Plaintiff and Class Members to adequately protect their personal data and to provide timely and accurate notice of the Data Breach to Plaintiff and Class Members;

- whether Defendant breached its duties to protect the personal data of Plaintiff and Class Members by failing to provide adequate data security and failing to provide timely and adequate notice of the Data Breach to Plaintiff and the Class;
- whether Defendant's conduct was negligent;
- whether Defendant knew or should have known that its computer systems were vulnerable to attack;
- whether Defendant's conduct, including its failure to act, resulted in or was the proximate cause of the Data Breach of its systems, resulting in the loss of Class Members' personal data;
- whether Defendant wrongfully or unlawfully failed to inform Plaintiff and Class Members that it did not maintain computers and security practices adequate to reasonably safeguard customers' personal data;
- whether Defendant should have notified the public, Plaintiff, and Class Members immediately after it learned of the Data Breach;
- whether Plaintiff and Class Members suffered injury, including ascertainable losses, as a result of Defendant's conduct (or failure to act);
- whether Plaintiff and Class Members are entitled to recover damages; and
- whether Plaintiff and Class Members are entitled to declaratory relief and equitable relief, including injunctive relief, restitution, disgorgement, and/or other equitable relief.

75. ***Typicality***. Plaintiff's claims are typical of the claims of the Class in that Plaintiff, like all Class Members, had their personal data compromised, breached, and stolen in the Data Breach. Plaintiff and all Class Members were injured through the uniform misconduct of

Defendant, described in this Complaint, and assert the same claims for relief.

76. ***Adequacy***. Plaintiff and counsel will fairly and adequately protect the interests of the Class. Plaintiff retained counsel who are experienced in Class action and complex litigation. Plaintiff haves no interests that are antagonistic to, or in conflict with, the interests of other Class Members.

77. ***Superiority***. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Moreover, absent a class action, most Class Members would find the cost of litigating their claims prohibitively high and would therefore have no effective remedy, so that in the absence of class treatment, Defendant's violations of law inflicting substantial damages in the aggregate would go unremedied without certification of the Class. Plaintiff and Class Members have been harmed by Defendant's wrongful conduct and/or action. Litigating this action as a class action will reduce the possibility of repetitious litigation relating to Defendant's conduct and/or inaction. Plaintiff knows of no difficulties that would be encountered in this litigation that would preclude its maintenance as a class action. Class certification is appropriate under Fed. R. Civ. P. 23(b)(1)(A), in that the prosecution of separate actions by the individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a class action conserves judicial resources and the parties' resources and protects the rights of each Class member. Specifically, injunctive relief could be entered in multiple cases, but the ordered relief may vary, causing Defendant to have to choose between differing means of upgrading its data security infrastructure and choosing the court order with which to comply. Class action status is

also warranted because prosecution of separate actions by the Class Members would create the risk of adjudications with respect to individual Class Members that, as a practical matter, would be dispositive of the interests of other members not parties to this action, or that would substantially impair or impede their ability to protect their interests.

78. Class certification, therefore, is appropriate under Fed. R. Civ. P. 23(b)(3), because the above common questions of law or fact predominate over any questions affecting individual Class Members, and a class action is superior to other available methods for the fair and efficient adjudication of this controversy.

79. Particular issues are also appropriate for certification under Fed. R. Civ. P. 23(c)(4) because the claims present particular, common issues, the resolution of which would materially advance the resolution of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

(a) Whether Plaintiff's and Class Members' PII and PHI were accessed, compromised, or stolen in the Data Breach;

(b) Whether (and when) Defendant knew about the Data Breach before it notified Plaintiff and Class Members and whether Defendant failed to timely notify Plaintiff and Class Members of the Data Breach;

(c) Whether Defendant owed a legal duty to Plaintiff and the Class;

(d) Whether Defendant failed to take reasonable steps to safeguard the PII and PHI of Plaintiff and Class Members;

(e) Whether Defendant failed to adequately monitor its data security systems;

(f) Whether Defendant failed to comply with its applicable laws, regulations, and industry standards relating to data security;

(g) Whether Defendant knew or should have known that it did not employ reasonable measures to keep Plaintiff's and Class members' PII or PHI secure;

(h) Whether Defendant's adherence to HIPAA regulations, FTC data security obligations, industry standards, and measures recommended by data security experts would have reasonably prevented the Data Breach.

80. Class certification is also appropriate under Fed. R. Civ. P. 23(b)(2). Defendant, through its uniform conduct, acted or failed and refused to act on grounds generally applicable to the Class as a whole, making injunctive and declaratory relief appropriate to the Class as a whole. Moreover, Defendant continues to maintain its inadequate security practices, retains possession of Plaintiff's and Class Members' PII and PHI, and has not been forced to change its practices or to relinquish PII and PHI by nature of other civil suits or government enforcement actions, thus making injunctive and declaratory relief a live issue and appropriate to the Class as a whole.

COUNT I
Negligence

81. Plaintiff incorporates paragraphs 1-80 of the Complaint as if fully set forth herein.

82. Plaintiff and Class Members were required to submit non-public PII and PHI to Defendant in order to obtain prescription medication services.

83. By collecting, storing, and using Plaintiff's and Class Members' PII and PHI, Defendant owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, securing, deleting, protecting, and safeguarding the sensitive PII and PHI it received from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

84. Defendant was required to prevent foreseeable harm to Plaintiff and Class Members, and therefore had a duty to take reasonable steps to safeguard their sensitive PII and PHI from unauthorized release or theft. More specifically, this duty included: (1) exercising

reasonable care in the hiring, training, and/or supervision of its employees and agents entrusted with access to Plaintiff's and Class Members' PII and PHI; (2) designing, maintaining, and testing Defendant's data security systems and data storage architecture to ensure Plaintiff's and Class Members' PII and PHI were adequately secured and protected; (3) implementing processes that would detect an unauthorized breach of Defendant's security systems and data storage architecture in timely and adequate manner; (4) timely acting on all warnings and alerts, including public information, regarding Defendant's security vulnerabilities and potential compromise of the PII and PHI of Plaintiff and Class Members; (5) maintaining data security measurers consistent with industry standards and applicable federal and state laws and other requirements; and (6) timely and adequately informing Plaintiff and Class Members if and when a data breach occurred to prevent foreseeable harm to them, notwithstanding undertaking (1)-(5) above.

85. Defendant had a common law duty to prevent foreseeable harm to Plaintiff and Class Members. The duty existed because Plaintiff and Class Members were the foreseeable and probable victims of any inadequate hiring, training, supervision, and security practices of Defendant in its affirmative collection of PII and PHI from Plaintiff and Class Members. In fact, not only was it foreseeable that Plaintiff and Class Members would be harmed by the failure to protect their PII and PHI because hackers routinely attempt to steal such information for use in nefarious purposes, Defendant knew that it was more likely than not Plaintiff and Class Members would be harmed as a result.

86. Defendant's duties to use reasonable security measures also arose as a result of the special relationship that existed between it, on the one hand, and Plaintiff and Class Members, on the other hand. This special relationship, recognized in laws and regulations, arose because Plaintiff and Class Members entrusted Defendant with their PII and PHI by virtue of receiving

health benefits through Defendant. Defendant alone could have ensured that its security systems and data storage architecture were sufficient to prevent or minimize the Data Breach.

87. The injuries suffered by Plaintiff and the Class Members were proximately and directly caused by Defendant's failure to exercise reasonable care in the hiring, training, and/or supervision of its employees and agents, as well as the failure to follow reasonable security standards to protect Plaintiff and the Class Members' PII and PHI.

88. When individuals have their personal information stolen, they are at substantial risk for imminent identity theft, and need to take steps to protect themselves, including, for example, buying credit monitoring services and purchasing or obtaining credit reports to protect themselves from identity theft.

89. If Defendant had taken reasonable security measures and/or exercised reasonable care in the hiring, training, and supervision of its employees and agents, data thieves would not have been able to take the personal information of Plaintiff and the Class Members. The policy of preventing future harm weighs in favor of finding a special relationship between Defendant and Plaintiff and the Class. If companies are not held accountable for failing to take reasonable security measures to protect the sensitive PII and PHI in their possession, they will not take the steps that are necessary to protect against future security breaches.

90. Defendant owed a duty to timely disclose the material fact that Defendant's computer systems and data security practices were inadequate to safeguard users' Sensitive Information from theft.

91. Defendant breached these duties through the conduct alleged in the Complaint by, including without limitation, failing to protect the PII and PHI in its possession; failing to maintain adequate computer systems and data security practices to safeguard the PII and PHI in its

possession; allowing unauthorized access to Plaintiff's and Class Members' PII and PHI; failing to disclose the material fact that Defendant's computer systems and data security practices were inadequate to safeguard the PII and PHI in its possession from theft; and failing to disclose in a timely and accurate manner to Plaintiff and Class Members the material fact of the Data Breach.

92. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and Class Members, their PII and PHI would not have been compromised. And as a direct and proximate result of Defendant's failure to exercise reasonable care and use commercially reasonable security measures, the PII and PHI of Plaintiff and the Class Members were accessed by ill-intentioned criminals who could and will use the information to commit identity or financial fraud. Plaintiff and Class Members face the imminent, certainly impending and substantially heightened risk of identity theft, fraud, and further misuse of their personal data.

93. It was foreseeable that Defendant's failure to exercise reasonable care in the hiring, training, and supervision of its employees and agents and to safeguard the PII and PHI in its possession or control would lead to one or more types of injury to Plaintiff and Class Members. And the Data Breach was foreseeable given the known, high frequency of cyberattacks and data breaches in the healthcare industry.

94. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have suffered, and continue to suffer, damages arising from the breach as described herein and are entitled to compensatory, consequential, and nominal damages in an amount to be proven at trial.

95. Such injuries include those described above, including: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary

loss and economic harm; loss of value of the compromised PII and PHI; illegal sale of the compromised PII and PHI on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach investigating the nature of the Data Breach, reviewing bank statements, payment card, statements, insurance statements, and credit reports; expenses and time spent initiating fraud alerts, decreased credit scores and ratings; lost time; other economic harm; and emotional distress.

COUNT II
Negligence *Per Se*

96. Plaintiff incorporates paragraphs 1-94 of the Complaint as if fully set forth herein.

97. Plaintiff and Class Members were required to provide non-public PII and PHI in order to obtain medical services and prescription medications.

98. Pursuant to Section 5 of the FTC Act, 15 U.S.C. §45, Defendant had a duty to provide fair and adequate computer systems and data security to safeguard the PII of Plaintiff and Class Members.

99. The FTC Act prohibits "unfair . . . practices in or affecting commerce," which the FTC has interpreted to include businesses' failure 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. In addition, individual states have enacted statutes based upon the FTC Act that also created a duty.

100. Pursuant to the Gramm-Leach-Bliley Act, Defendant had a duty to protect the security and confidentiality of Plaintiff's and Class Members' PII. *See* 15 U.S.C. § 6801.

101. Pursuant to the Fair Credit Reporting Act ("FCRA"), Defendant had a duty to adopt, implement, and maintain adequate procedures to protect the security and confidentiality of Plaintiff's and Class Members' PII. *See* 15 U.S.C. § 1681(b).

102. Defendant solicited, gathered, and stored PII and PHI of Plaintiff and the Class Members to facilitate transactions which affect commerce.

103. Defendant violated the FTC Act (and similar state statutes), HIPAA, the FCRA, and the Graham-Leach-Bliley Act by failing to use reasonable measures to protect PII and PHI of Plaintiff and Class Members and not complying with applicable industry standards, as described herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII and PHI obtained and stored and the foreseeable consequences of a data breach on Defendant's systems.

104. Defendant's violation of the FTC Act (and similar state statutes) as well as its violations of the FCRA, and the Graham-Leach-Bliley Act constitutes negligence *per se*.

105. Plaintiff and the Class Members are within the class of persons that the FTC Act (and similar state statutes), the FCRA, and the Graham-Leach-Bliley Act were intended to protect.

106. The harm that occurred as a result of the breach is the type of harm the FTC Act (and similar state statutes), as well as the FCRA and the Graham-Leach-Bliley Act were 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 caused the same harm as that suffered by Plaintiff and the Class Members.

107. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and Class Members have suffered, and continue to suffer, damages arising from the breach as described herein and are entitled to compensatory, consequential, and nominal damages in an amount to be proven at trial.

108. Such injuries include those described above, including: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary

loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of value of the compromised PII and PHI; illegal sale of the compromised PII and PHI on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach investigating the nature of the Data Breach, reviewing bank statements, payment card, statements, insurance statements, and credit reports; expenses and time spent initiating fraud alerts, decreased credit scores and ratings; lost time; other economic harm; and emotional distress.

COUNT III
Declaratory Judgment

109. Plaintiff incorporates paragraphs 1-107 of the Complaint as if fully set forth herein.

110. 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.

111. 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.

112. 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 Plaintiff's and Class Members' PII and PHI.

113. 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.

114. If an injunction is not issued, Plaintiff and Class Members will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach of Defendant. The risk of another such breach is real, immediate, and substantial. If another breach occurs, Plaintiff 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.

115. The hardship to Plaintiff 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 at Defendant, Plaintiff 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 a pre-existing legal obligation to employ such measures.

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

RELIEF REQUESTED

Plaintiff, individually and on behalf of the proposed Class, requests that the Court:

1. Certify this case as a class action on behalf of the Class, defined above, appoint Plaintiff as Class representative, and appoint the undersigned counsel as class counsel;
2. Award declaratory, injunctive, and other equitable relief as is necessary to protect the interests of Plaintiff and other Class Members;
3. Award restitution; compensatory, consequential, and general damages, including nominal damages as allowed by law in an amount to be determined at trial or by this Court;
4. Award Plaintiff and Class Members their reasonable litigation expenses and attorneys' fees to the extent allowed by law;
5. Award Plaintiff and Class Members pre- and post-judgment interest, to the extent allowable; and
6. Award such other and further relief as equity and justice may require.

JURY TRIAL DEMANDED

Pursuant to Federal Rule of Civil Procedure 38(b), Plaintiff demands a trial by jury of any and all issues in this action so triable as of right.

Respectfully submitted,

/s/ John A. Yanchunis
John A. Yanchunis
Ryan D. Maxey
MORGAN & MORGAN
COMPLEX LITIGATION GROUP
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
(813) 223-5505
jyanchunis@ForThePeople.com
rmaxey@ForThePeople.com

Terence R. Coates (*Pro Hac Vice* Forthcoming)
Dylan J. Gould (*Pro Hac Vice* Forthcoming)
MARKOVITS, STOCK & DEMARCO, LLC
3825 Edwards Road, Suite 650
Cincinnati, OH 45209
Phone: (513) 651-3700
Fax: (513) 665-0219
tcoates@msdlegal.com
dgould@msdlegal.com

Counsel for Plaintiff and the Class