Exhibit A-3

UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF FLORIDA
ORLANDO DIVISION

BONNIE GILBERT, WENDY BRYAN, PATRICIA WHITE, DAVID GATZ, CRYSTAL HULLET, LORI GRADER, DARYL SWANSON, STEPHEN GABBARD, ALICIA DUNN, and on behalf of themselves and all others similarly situated, **Plaintiffs,** **v.** **BIOPLUS SPECIALTY PHARMACY SERVICES, LLC,** **Defendant.**	Case No. 6:21-cv-2158-RBD-DCI **CONSOLIDATED CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiffs Bonnie Gilbert, Wendy Bryan, Patricia White, David Gatz, Crystal Hullet, Lori Grader, Daryl Swanson, Stephen Gabbard, and Alicia Dunn, (collectively, "Plaintiffs"), by and through their attorneys, upon personal knowledge as to their own acts and experiences, investigation of their counsel, and upon information and belief as to all other matters, allege 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 complex chronic medical conditions

such as cancer, infusion, multiple sclerosis, hepatitis C.

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"), including 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. The full extent of the types of Sensitive Information, the scope of the breach, and the root cause of the Data Breach is all within the exclusive control of Defendant and its agents, counsel, and forensic security vendors at this phase of litigation.

4. BioPlus has admitted that the Sensitive Information of its patients was accessed by cybercriminals and that this data was unencrypted.[1]

5. In total, the Data Breach exposed the Sensitive Information of approximately 350,000 current and former BioPlus patients and customers ("Class

[1] 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) (emphasis added). Defendant notified the California Attorney General of the Data Breach on or about May 28, 2021, evidencing that the exposed data was unencrypted. https://oag.ca.gov/ecrime/databreach/reports/sb24-548450 (last visited March 27, 2022).

Members").[2]

6. BioPlus is responsible for allowing this Data Breach because of multiple acts of negligence, including but not limited to its: failure to design, implement, and maintain reasonable data security systems and safeguards; failure to exercise reasonable care in the hiring, supervision, and training of its employees and agents and vendors; failure to comply with industry-standard data security practices; and failure to comply with federal and state laws and regulations that govern data security and privacy practices and are intended to protect the type of Sensitive Information at issue in this action.

7. Despite its role in managing so much Sensitive Information, Defendant failed to take basic security measures such as encrypting its data. Moreover, Defendant failed to recognize and detect that unauthorized third parties had accessed its network and, upon information and belief, further failed to recognize that substantial amounts of data had been compromised, and more likely than not, exfiltrated and stolen. Had Defendant not committed the acts of negligence described herein, it would have discovered the Data Breach sooner – and/or prevented the invasion and theft altogether.

8. Defendant owed numerous statutory, regulatory, contractual, and common law duties to Plaintiffs and the Class Members to protect and keep their

[2] https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited March 27, 2022).

Sensitive Information confidential, safe, secure, and protected from unauthorized disclosure, access, or unconsented exfiltration, including duties under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and The Federal Trade Commission Act, 15 U.S.C. § 45. ("FTCA").

9. Moreover, by obtaining, collecting, using, and deriving benefit from Plaintiffs' and Class Members' Sensitive Information, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiffs' and Class Members' Sensitive Information from disclosure.

10. As patients and/or customers of Defendant, Plaintiffs and Class Members were required to provide their Sensitive Information to Defendants directly or indirectly through their treating physicians or health insurance providers.

11. In acquiring and maintaining Plaintiffs' and Class Members' Sensitive Information, Defendant expressly and impliedly promised to safeguard Plaintiffs' and Class Members' Sensitive Information.

12. Plaintiffs and Class Members reasonably relied upon Defendant to maintain the security and privacy of the Sensitive Information entrusted to it. Plaintiffs and Class Members further relied on Defendant to keep their Sensitive Information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this

information.

13. Plaintiffs and Class Members reasonably expected and understood that Defendant would ensure that it would comply with its numerous duties, promises, and obligations to keep Plaintiffs' Sensitive Information secure and safe from unauthorized access.

14. Plaintiffs and Class Members would not have paid the amounts they paid for pharmacy services, had they known their information would be maintained using inadequate data security systems. Defendant, however, breached their duties, promises, and obligations, and Defendants' failures increased the risk that Plaintiffs' Sensitive Information would be compromised in the event of a likely cyberattack.

0. 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, as this Data Breach was highly foreseeable.

15. Upon information and belief, as a result of Defendant's failures to protect the Sensitive Information of Plaintiffs and Class Members, their Sensitive Information was disclosed, accessed, downloaded, and/or exfiltrated by malicious cyber criminals, who targeted that information through their wrongdoing. As a direct and proximate result, Plaintiffs and the Class Members are now at a significant present and future risk of identity theft, financial fraud,

health care identity fraud, and/or other identity-theft or fraud, imminently and for years to come.

17. In the months and years following the Data Breach, Plaintiffs and the other Class Members will experience numerous types of harms as a result of Defendant's ineffective and inadequate data security measures. Some of these harms will likely include fraudulent charges on financial accounts, opening fraudulent financial accounts, acquiring medical procedures and prescriptions ordered in patients' names, and targeted advertising without patient consent.

18. Plaintiffs and Class Members have also now lost the economic value of their Sensitive Information. Indeed, there is both a healthy black market and a legitimate market for that Sensitive Information. Just as Plaintiffs' and Class Members' Sensitive Information were stolen, *inter alia*, because of its inherent value in the black market, the inherent value of Plaintiffs' and the Class Members' Sensitive Information in the legitimate market is now significantly and materially decreased.

19. Plaintiffs and Class Members have suffered numerous actual and imminent injuries as a direct result of the Data Breach, including: (a) theft of their Sensitive Information; (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) the diminution in value of their personal data; (h) the loss of value of the bargain for paying for services that required entrusting their Sensitive Information to Defendant with the mutual understanding that Defendant would safeguard the Sensitive Information against improper disclosure, misuse, and theft; and (h) the continued risk to their Sensitive Information, 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 Plaintiffs' and Class Members' Sensitive Information.

20. Plaintiffs seek to remedy these harms, and to prevent their future occurrence, on behalf of themselves and all similarly situated persons whose Sensitive Information were compromised as a result of the Data Breach.

21. Accordingly, Plaintiffs, on behalf of themselves and other Class Members, assert claims for negligence (Count I); negligence *per se* (Count II); breach of fiduciary duty (Count III); breach of contract (IV); breach of implied contract (Count V); violations of Florida's Deceptive and Unfair Trade Practices

Act, Fla. Stat. § 501.201, *et seq.* (Count VI); violations of New Jersey's Consumer Fraud Act, N.J. Rev. Stat. § 56:8-1, *et seq.* (Count VII); violations of the Connecticut Unfair Trade Practices Act, Con. Gen, Stat. §42-110, *et seq.* (Count VIII); violations of O.C.G.A. § 13-6-11 (Count IX); violations of the North Carolina Deceptive Trade Practices Act, N.C. Gen. Stat. § 75-1.1, *et seq.* (Count X); and declaratory judgment (Count XI). Plaintiffs seek injunctive relief, declaratory relief, monetary damages, and all other relief as authorized in equity or by law.

THE PARTIES

Plaintiff Bonnie Gilbert

22. Plaintiff Bonnie Gilbert is a resident and citizen of the State of Georgia and intends to remain domiciled in and a citizen of the State of Georgia.

23. Plaintiff Gilbert received a letter dated December 10, 2021 from Defendant concerning the Data Breach. The letter stated that unauthorized actors accessed BioPlus's network containing 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.

Plaintiff Wendy Bryan

24. Plaintiff Wendy Bryan is a resident and citizen of New Jersey. Ms. Bryan has resided in the state of New Jersey for nearly fifty years and owns a home within the state. Plaintiff Bryan intends to remain in New Jersey indefinitely.

25. Plaintiff Bryan received a letter dated December 10, 2021 from Defendant concerning the Data Breach. The letter stated that unauthorized actors accessed BioPlus's network containing 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.

Plaintiff Patricia White

26. Plaintiff Patricia White is a resident and citizen of Connecticut. Plaintiff White has resided in Connecticut for her entire life, has a registered automobile in the state of Connecticut, and has been a member of local civic groups in the state of Connecticut for nearly three decades. She intends to remain in Connecticut indefinitely.

27. Plaintiff White received a letter dated December 10, 2021 from Defendant concerning the Data Breach. The letter stated that unauthorized actors accessed BioPlus's network containing 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.

Plaintiff David Gatz

28. Plaintiff David Gatz is a citizen and resident of Florida. He does not intend to move to another state in the immediate future and intends to remain domiciled and a resident and citizen of Florida.

29. Plaintiff Gatz received a letter dated December 10, 2021 from Defendant concerning the Data Breach. The letter stated that unauthorized actors accessed BioPlus's network containing 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.

Plaintiff Crystal Hullet

30. Plaintiff, Crystal Hullet, is a resident and citizen of the state of North Carolina and intends to remain domiciled in and a citizen of North Carolina.

31. On or about December of 2021, Plaintiff Hullet received notice from BioPlus that unauthorized actors accessed BioPlus's network containing her Sensitive Information.

Plaintiff Lori Grader

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

33. Plaintiff Grader received a letter dated December 10, 2021 from Defendant concerning the Data Breach. The letter stated that unauthorized actors gained access to BioPlus's network containing 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.

Plaintiff Daryl Swanson

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

35. Plaintiff Swanson received a letter dated December 10, 2021 from Defendant concerning the Data Breach. The letter stated that unauthorized actors gained access to BioPlus's network containing 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.

Plaintiff Stephen Gabbard

36. Plaintiff Stephen Gabbard is a resident and citizen of Kentucky. He does not intend to move to a different state in the immediate future and intends to remain domiciled and a resident and citizen of the Commonwealth of Kentucky.

37. Plaintiff received a letter dated December 10, 2021 from Defendant concerning the Data Breach. The letter stated that unauthorized actors gained access to BioPlus's network containing 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.

Plaintiff Alicia Dunn

38. Plaintiff Alicia Dunn is a resident and citizen the State of North Carolina and intends to remain domiciled in and a citizen of the State of North Carolina.

39. Plaintiff Dunn received a letter dated December 10, 2021 from Defendant concerning the Data Breach. The letter stated unauthorized actors gained access to BioPlus's network containing 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.

Defendant BioPlus

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

41. According to one of its recent business filings 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.

42. 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."[3]

JURISDICTION & VENUE

43. 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 is a citizen of the State of Georgia and Defendant is a citizen of the State of Florida and State

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

of Washington. Accordingly, minimal diversity under CAFA exists because Defendant as an LLC is a citizen of the State of Florida and the State of Washington and Plaintiff Gilbert is a citizen of the State of Georgia.

44. 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.

45. Venue is proper in this District under 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 emanated from activities within this District, and Defendant conducts substantial business in this District

FACTUAL ALLEGATIONS

The Data Breach

46. 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.

47. 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.

48. The letters received by Plaintiffs and Class Members indicate that the following Sensitive Information was exposed in the breach: patient names, dates of birth, addresses, Social Security numbers, medical record numbers, current/former health plan member ID numbers, claims information, diagnoses, and/or prescription information.

49. The notification letters provided to Plaintiffs 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. Even the notice letters to Class Members, such as the one received by Plaintiff Gilbert, recognize that "this incident may have caused" the letter recipients to suffer "inconvenience or concern."

50. Patients whose Social Security numbers were determined to be exposed in the Data Breach, such as Plaintiffs, were offered a one or two-year subscription to Experian credit monitoring and identity protection services. BioPlus has not offered to extend this credit monitoring longer for an amount of time sufficient to protect Plaintiffs and Class Members from the present, imminent, and substantially increased risk of fraud and identity theft both now and for years to come.

51. But for Defendant's failure to take reasonable steps to secure Plaintiffs' 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.

52. The Sensitive Information in the Data Breach was unencrypted and was exfiltrated by the hackers who accessed Defendant's system.

53. The Data Breach notices BioPlus sent to Plaintiffs and Class Members indicate that BioPlus's cybersecurity at the time of the Data Breach was deficient. Notably, BioPlus informed Plaintiffs and Class Members that it was required to implement new safeguards and technical security measures to adequately protect its systems after the Data Breach. This was too little, too late as BioPlus's deficient cybersecurity at the time of the Data Breach caused Plaintiffs' and Class Members' Sensitive Information to be accessed and exfiltrated by hackers. Furthermore, it was deficient to hold Plaintiffs and Class Members' Sensitive Information in an unencrypted form.

54. It is common sense that the criminal(s) that breached Defendant's systems and acquired the victims' Sensitive Information 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 Sensitive Information to other individuals intending to commit fraud, theft, and other crimes. Given that this is the reason such Sensitive Information are sought by criminals, it is similarly common sense that Plaintiffs and the Class Members have already suffered injury and face a substantial risk for

imminent and certainly impending future injury.

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

56. 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]

57. The physical, emotional, and social toll suffered (in addition to the financial toll) by identity theft victims cannot be understated.[6] "A 2016 Identity

---

[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 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.*

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]

58. 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.

59. 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.

60. 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.

---

[7] *Id.*

61. 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.

62. 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 Plaintiffs and the Class will continue and increase, and Plaintiffs 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.

63. Defendant is fully aware of how sensitive the Sensitive Information it stores and maintains is. It is also aware of how much Sensitive Information it collects, uses, and maintains from Plaintiffs and Class Members.

64. 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 Sensitive Information through its computer data and storage systems.

65. By requiring the production of, collecting, obtaining, using, and deriving benefits from Plaintiffs' and the Class Members' Sensitive Information, Defendant assumed certain legal and equitable duties, and it knew or should have known that it was responsible for the diligent protection of that Sensitive

Information it collected and stored.

66. 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.

67. 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.

68. 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]

69. Protenus, a healthcare compliance analytics firm, analyzed data breach incidents disclosed to the U.S. Department of Health and Human Services

---

[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.*

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]

70. 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

71. 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 information.[13]

---

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).

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).

72. 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 Sensitive Information to bad actors—would be exponentially higher today.

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

73. 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

[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).

most valuable to hackers.[15]

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

75. 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]

76. Criminals can, for example, use Social Security numbers to create false

---

[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).

[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).

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.

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

78. 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

---

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.

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).

PHI. In 2020, final payouts to hackers committing ransomware attacks involving PHI averaged $910,335.[20]

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

80. 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.

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

82. Because the information Defendant allowed to be compromised and taken is of such a durable and permanent quality, the harms to Plaintiffs and the Class will continue and increase, and Plaintiffs and Class Members will continue

[20] Jerich, *supra* n.12.
[21] *See* FBI, *supra* n.18.

to be at substantial risk for further imminent and future harm.

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

83. 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 Sensitive Information belonging to Plaintiffs and the Class Members, do not need to use the information to commit fraud immediately. The Sensitive Information can be used or sold for use years later, and often is.

84. Plaintiffs and Class Members are now at a significant risk of imminent and future fraud, misuse of their Sensitive Information, 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 away with misuse for years before healthcare-related fraud is spotted.

85. Plaintiffs and Class Members have suffered real and tangible losses, including but not limited to the loss in the inherent value of their Sensitive Information, 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.

86. Despite Defendant's egregious failure to protect Plaintiffs' Sensitive Information, it has only offered to provide them with trivial compensation or remedy, such as one or two years of credit monitoring or identity protection services.

PLAINTIFFS' EXPERIENCES

Plaintiff Bonnie Gilbert

87. Gilbert used BioPlus's services when she had a specialty prescription filled through her doctor's office. To receive services at BioPlus, Plaintiff Gilbert was required to provide her Sensitive Information directly to Defendant, which, upon information and belief, was provided by her treating physician, or health insurance, and was then entered into BioPlus's database and maintained by Defendant.

88. Plaintiff Gilbert greatly values her privacy and Sensitive Information, especially when receiving medical services. Prior to the Data Breach, Plaintiff took reasonable steps to maintain the confidentiality of her Sensitive Information.

89. Recognizing the substantial risk Plaintiff Gilbert faces from the Data Breach, Defendant provided Plaintiff Gilbert a one-year subscription to a credit monitoring service. However, Plaintiff Gilbert was forced to spend time signing up for this service. Moreover, Plaintiff Gilbert will be forced to incur additional

costs to maintain this service after her subscription expires in one year.

90. In addition, Plaintiff Gilbert 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 Gilbert has called ahead and given preauthorization. Plaintiff Gilbert will be forced to spend significant time in the future providing preauthorization for others to pick up her medication in an effort to prevent future healthcare identity theft.

91. Since learning of the Data Breach, Plaintiff Gilbert has spent significant time reviewing her financial accounts. Plaintiff Gilbert has also spent significant time speaking with her bank regarding her concerns about the Data Breach and traveling to and from her bank. After consulting with her bank, Plaintiff Gilbert decided that the safest option to protect herself from future fraud was to close her checking account and open a new one. As a result, Plaintiff Gilbert lost approximately $100 worth of new personalized checks that she purchased before learning of the Data Breach.

92. Since the Data Breach, Plaintiff Gilbert has received a significant amount of medical-related mail at her home address addressed to an unknown individual named "Lynn Yara." This mail was sent from several different insurance companies related to a Medicare application. She has spent several hours on the phone with these companies informing these companies that no

individual named "Lynn Yara" resides at her address, that she does not know Ms. Yara, and asking the companies to cease sending her mail addressed to this person.

93. After learning of the Data Breach, Plaintiff Gilbert implemented credit freezes with TransUnion, Equifax, and Experian. It took Plaintiff Gilbert significant time to implement the credit freeze with each of these three companies. The freezing of her credit will cause her future inconvenience and lost time as well.

94. The Data Breach has caused Plaintiff Gilbert to suffer significant fear, anxiety, stress, and sleep disruption, due to concerns for future identity theft.

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

Plaintiff Wendy Bryan

96. Plaintiff Bryan used BioPlus's services in 2021 when she had a specialty prescription filled through her doctor's office. To receive services at BioPlus, Plaintiff Bryan was required to provide her Sensitive Information directly to Defendant, which, upon information and belief, was provided by her treating physician, or health insurance, and was then entered into BioPlus's database and maintained by Defendant.

97. Plaintiff Bryan greatly values her privacy and Sensitive Information,

especially when receiving medical services. Prior to the Data Breach, Plaintiff Bryan took reasonable steps to maintain the confidentiality of her Sensitive Information.

98. Recognizing the substantial risk Plaintiff Bryant faces, the letter also offered one year of credit monitoring through Experian's IdentityWorks Credit 3B monitoring. Plaintiff has not accepted this offer due to a lack of trust with Defendant. The Experian credit monitoring would have shared Ms. Bryan's information with third parties and could not guarantee complete privacy of her Sensitive Information. Rather, Plaintiff Bryan incurred out of pocket expenses to subscribe to Life Lock at $191.92/year.

99. In addition, due to the Data Breach, Plaintiff Bryan has spent significant time reviewing her personal accounts and information, researching the Data Breach, and reviewing Equifax reports.

100. Learning that she was a victim of Data Breach caused her to become very upset. Plaintiff Bryan has also suffered from general nuisance and annoyance.

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

Plaintiff Patricia White

102. Plaintiff White's information was entered into BioPlus's systems in

2015 when a clerical error resulted in her prescription information from her doctor's office being sent to BioPlus instead of her in-network pharmacy. Plaintiff White corrected the clerical error and canceled the service from BioPlus.

103. However, BioPlus, without any medical or business purpose, and without Plaintiff White's consent, continued to hold her information in Defendant's systems, where her Sensitive Information remained vulnerable to foreseeable Data Breaches.

104. Recognizing the substantial risk Plaintiff White faces, the letter also offered two years of Experian IdentityWorks Credit 3B monitoring. Plaintiff White did not accept this offer because accepting the credit monitoring from BioPlus would have meant transmitting Sensitive Information back to Defendant after it had already demonstrated that it could not be trusted with such information.

105. Some of the damages that will likely occur with respect to Class Members have already manifested themselves in Plaintiff White's experience. For example, on or about November 30, 2021, Plaintiff White received a notification from her credit monitoring services through H &R Block that her information appeared on the dark web, where cyber-criminals trade sensitive patient information for use in phone, banking, and health insurance scams. Plaintiff White has notified her credit monitoring services of this breach and continues to monitor her accounts for suspicious activity.

106. Plaintiff White values the privacy of her personal information. Prior to the Data Breach, Plaintiff White took reasonable steps to maintain the confidentiality of her Sensitive Information.

107. She never consented to her information being transmitted to BioPlus's systems—or that BioPlus could maintain her Sensitive Information after resolving the mistaken prescription. Had she known her Sensitive Information would be maintained using inadequate storage methods that would lead to its misuse, she would have taken prior action to request the information be deleted from the BioPlus system.

108. Due to the Data Breach, Plaintiff White has spent significant time reviewing her personal accounts and implementing a credit freeze and fraud alert. This credit freeze will cause Plaintiff White to suffer additional lost time and inconvenience.

109. The Data Breach has caused Plaintiff White to suffer annoyance and general nuisance, which is compounded by the fact that BioPlus never should have had her Sensitive Information in the first place.

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

Plaintiff David Gatz

111. Upon information and belief, Plaintiff Gatz's Sensitive Information was provided indirectly to BioPlus, from a treating physician, or health insurance as part of Plaintiff's medical care.

112. Plaintiff Gatz greatly values his privacy and Sensitive Information, especially when receiving medical services. Prior to the Data Breach, Plaintiff Gatz took reasonable steps to maintain the confidentiality of his Sensitive Information.

113. Recognizing the substantial risk Plaintiff Gatz faces, Defendant provided Plaintiff Gatz a one-year subscription to a credit monitoring service. Plaintiff Gatz rejected this offer. Rather, he had previously enrolled in credit monitoring service with his bank that was unconnected to the Defendant. However, he has incurred out of pocket charges and will continue to incur a charge of $5-$7 per month for 5 years.

114. Moreover, since learning of the Data Breach, Plaintiff Gatz has spent several hours reviewing his bank statements and credit cards. Due to his concern for future identity theft and fraud, he has also taken steps to freeze bank debit cards and further requested that his bank cancel and issue new cards, thereby limiting his access to his bank funds in the short term.

115. The Data Breach has caused Plaintiff Gatz to suffer anxiety, mental anguish, and stress.

116. Plaintiff Gatz plans on taking additional time-consuming, yet necessary, steps to help mitigate the harm caused by the Data Breach.

Plaintiff Crystal Hullet

117. Plaintiff Hullet was a BioPlus customer prior to the Data Breach. As a condition of receiving BioPlus's services, BioPlus required Plaintiff Hullet to provide it with her Sensitive Information. As such, Plaintiff Hullet provided BioPlus her Sensitive Information to purchase BioPlus's services and medications, either directly or indirectly through her physician or health insurance, which was then entered into BioPlus's database and maintained by Defendant.

118. Plaintiff Hullet greatly values her privacy and Sensitive Information, especially when receiving medical services. Prior to the Data Breach, Plaintiff Hullet took reasonable steps to maintain the confidentiality of her Sensitive Information.

119. Recognizing the substantial risk Plaintiff Hullet faces, Defendant provided Plaintiff Hullet a one-year subscription to a credit monitoring service, which she accepted. 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.

120. In response, Plaintiff Hullet spent considerable time and effort

monitoring her accounts and credit reports to protect herself from additional identity theft. Plaintiff Hullet fears for her personal financial security and uncertainty over what Sensitive Information was revealed in the Data Breach and how that information may be used to harm her.

121. Since the Data Breach, Plaintiff Hullet has also received a significant increase in spam calls that cause nuisance, annoyance, and a loss of time and attention.

122. Plaintiff Hullet plans on taking additional time-consuming, yet necessary, steps to help mitigate the harm caused by the Data Breach.

Plaintiff Lori Grader

123. Plaintiff Grader used BioPlus's services when she had a specialty prescription filled through her doctor's office. As a condition of receiving services at BioPlus, upon information and belief, Plaintiff Grader's Sensitive Information was provided by Plaintiff's physicians or her health insurance, as part of her medical services, which was then entered into BioPlus's database and maintained by Defendant.

124. Plaintiff Grader greatly values her privacy and Sensitive Information, especially when receiving medical services. Prior to the Data Breach, Plaintiff Grader took reasonable steps to maintain the confidentiality of her Sensitive Information.

125. Recognizing the substantial, present and substantially increased future 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, and has not elected this service to date. Moreover, she would 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.

126. Since learning of the Data Breach, Plaintiff Grader has spent time researching the Data Breach and researching protective steps to prevent or mitigate the risk of identity theft. She has also spent time reviewing her bank statements and credit cards at a more frequent interval than she did previously. And she has spent significant time speaking with her bank regarding her concerns about the Data Breach.

127. 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, implementing identity theft protection, monitoring her credit and identity, and checking her financial accounts.

Plaintiff Daryl Swanson

128. Plaintiff Swanson used BioPlus's services when he had a specialty prescription filled through his doctor's office. As a condition to receive services at BioPlus, upon information and belief, Plaintiff Swanson's Sensitive Information

was provided by himself, his physicians, or his medical insurance as part of his medical services, which was then entered into BioPlus's database and maintained by Defendant.

129. Plaintiff Swanson greatly values his privacy and Sensitive Information, especially when receiving medical services. Prior to the Data Breach, Plaintiff Swanson took reasonable steps to maintain the confidentiality of his Sensitive Information.

130. Recognizing the substantial risk Plaintiff Swanson faces, Defendant provided him a one-year subscription to a credit monitoring service, which he enrolled in. 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.

131. In addition, Plaintiff Swanson has received an increase in spam text messages regarding Medicare and medical insurance that has caused nuisance, annoyance, and an additional loss of time and attention.

132. 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.

Plaintiff Stephen Gabbard

133. As a condition to receiving services at BioPlus, upon information and belief, Plaintiff Gabbard's Sensitive Information was provided by Plaintiff Gabbard's physicians or health insurance as part of his medical services, which was then entered into BioPlus's database and maintained by Defendant.

134. Plaintiff Gabbard greatly values his privacy and Sensitive Information, especially when receiving medical services. Before the Data Breach, Plaintiff Gabbard took reasonable steps to maintain the confidentiality of his Sensitive Information.

135. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Gabbard faces, Defendant provided Plaintiff Gabbard a one-year subscription to a credit monitoring service, which Plaintiff did not accept.

136. Since learning of the Data Breach, Plaintiff Gabbard has spent hours reviewing his bank statements and credit cards for any fraud or suspicious activity.

137. The Data Breach has caused Plaintiff Gabbard to suffer general nuisance and annoyance.

138. Plaintiff Gabbard plans on taking additional time-consuming, yet necessary, steps to help mitigate the harm caused by the Data Breach, including continually reviewing his depository, credit, and other accounts for any

unauthorized activity.

Plaintiff Alicia Dunn

139. Plaintiff Dunn used BioPlus's services when she had a specialty prescription filled through her doctor's office. As a condition to receiving services at BioPlus, upon information and belief, Plaintiff Dunn's Sensitive Information was provided by Plaintiff or by Plaintiff's physicians, or her health insurance, as part of her medical services, which was then entered into BioPlus's database and maintained by Defendant.

140. Plaintiff Dunn greatly values her privacy and Sensitive Information, especially when receiving medical services. Prior to the Data Breach, Plaintiff Dunn took reasonable steps to maintain the confidentiality of her Sensitive Information.

141. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Dunn faces, Defendant provided Plaintiff Dunn a one-year subscription to a credit monitoring service. However, Plaintiff Dunn did not sign up for the program, as she has an inherent mistrust of the Defendant following the Data Breach.

142. In October 2021, Plaintiff Dunn experienced actual identity fraud with an unauthorized $30 charge on her debit card for her checking account. As a result, she was required to obtain a new debit card, which took about a month to receive

and limited her access to her checking account. She believes the unauthorized $30 charge on her debit card is a result of the Data Breach given that it occurred relatively soon after the Data Breach, and she had no other previous fraudulent charges on her debit card.

143. Since learning of the Data Breach, Plaintiff Dunn has spent time reviewing her bank statements and credit cards. She spent time every day for roughly two weeks attempting to procure a new debit card from her bank, which she believes was 30-45 minutes every day for two weeks totaling 7-8 hours speaking with her bank.

144. She also has experienced an increase in phone calls regarding medical insurance products and/or plan offerings since the Data Breach. Furthermore, Plaintiff Dunn has received an increase of other spam calls and emails after the Data Breach.

145. The Data Breach has caused Plaintiff Dunn to suffer significant fear, anxiety, and stress, which has been compounded by the fact that BioPlus has not been forthright with information about the Data Breach.

146. Plaintiff Dunn plans on taking additional time-consuming, yet necessary, steps to help mitigate the harm caused by the Data Breach, including continually reviewing her depository, credit, and other accounts for any unauthorized activity.

CLASS ACTION ALLEGATIONS

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

> **All persons who reside in the United States who received or were otherwise sent notice that their data was potentially compromised due to the Data Breach.**

148. Plaintiffs also seek to certify the following subclasses:

> **Connecticut Subclass: All residents of Connecticut who received or were otherwise sent notice that their data was potentially compromised due to the Data Breach.**
>
> **Florida Subclass: All residents of Florida who received or were otherwise sent notice that their data was potentially compromised due to the Data Breach.**
>
> **Georgia Subclass: All residents of Georgia who received or were otherwise sent notice that their data was potentially compromised due to the Data Breach.**
>
> **New Jersey Subclass: All residents of New Jersey who received or were otherwise sent notice that their data was potentially compromised due to the Data Breach.**
>
> **North Carolina Subclass: All residents of North Carolina who received or were otherwise sent notice that their data was potentially compromised due to the Data Breach.**

149. Excluded from the Nationwide Class and Subclasses are Defendant; officers and directors 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.

150. Plaintiffs reserve the right to modify and/or amend the Nationwide Class and Subclass definitions, including but not limited to creating additional subclasses, as necessary.

151. Certification of Plaintiffs' claims for class-wide treatment is appropriate because Plaintiffs 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.

152. 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.

153. Numerosity. The Class and Subclasses are 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. Upon information and belief, each subclass contains a minimum of 50 individuals.

154. Commonality and Predominance. There are numerous questions of law and fact common to Plaintiffs 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 Plaintiffs and Class Members to adequately protect their personal data and to provide timely and accurate notice of the Data Breach to Plaintiffs and Class Members;
- whether Defendant breached its duties to protect the personal data of Plaintiffs and Class Members by failing to provide adequate data security and failing to provide timely and adequate notice of the Data Breach to Plaintiffs 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 Plaintiffs 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 Plaintiffs and Class Members suffered injury, including ascertainable losses, as a result of Defendant's conduct (or failure to act);
- whether Plaintiffs and Class Members are entitled to recover damages; and,
- whether Plaintiffs and Class Members are entitled to declaratory relief and equitable relief, including injunctive relief, restitution, disgorgement, and/or other equitable relief.

155. ***Typicality***. Plaintiffs' 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. Plaintiffs and all Class Members were injured through the uniform misconduct of Defendant, described in this Complaint, and assert the same claims for relief.

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

157. ***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. Plaintiffs 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. Plaintiffs know 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.

158. 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.

159. 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 Plaintiffs' and Class Members' Sensitive Information were accessed, compromised, or stolen in the Data Breach;

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

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

(d) Whether Defendant failed to take reasonable steps to safeguard the Sensitive Information of Plaintiffs 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 Plaintiffs' 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.

160. 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 Plaintiffs' and Class Members' Sensitive Information, and has not been forced to change its practices or to relinquish Sensitive Information 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
(On behalf of Plaintiffs and the Nationwide Class)

161. Plaintiffs incorporate paragraphs 1-160 of the Complaint as if fully set forth herein.

162. Plaintiffs and Class Members were required to submit non-public Sensitive Information to Defendant in order to obtain prescription medication services.

163. By collecting, storing, and using Plaintiffs' and Class Members' Sensitive Information, Defendant owed a duty to Plaintiffs and Class Members to

exercise reasonable care in obtaining, securing, deleting, protecting, and safeguarding the Sensitive Information it received from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

164. Defendant was required to prevent foreseeable harm to Plaintiffs and Class Members, and therefore had a duty to take reasonable steps to safeguard their Sensitive Information 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 Plaintiffs' and Class Members' Sensitive Information; (2) designing, maintaining, and testing Defendant's data security systems and data storage architecture to ensure Plaintiffs' and Class Members' Sensitive Information 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 Sensitive Information of Plaintiffs 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 Plaintiffs and Class Members if and when a data breach occurred to prevent foreseeable harm to them, notwithstanding undertaking (1)-

(5) above.

165. Defendant had a common law duty to prevent foreseeable harm to Plaintiffs and Class Members. The duty existed because Plaintiffs 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 Sensitive Information from Plaintiffs and Class Members. In fact, not only was it foreseeable that Plaintiffs and Class Members would be harmed by the failure to protect their Sensitive Information because hackers routinely attempt to steal such information for use in nefarious purposes, Defendant knew that it was more likely than not Plaintiffs and Class Members would be harmed as a result.

166. 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 Plaintiffs and Class Members, on the other hand. This special relationship, recognized in laws and regulations, arose because Plaintiffs and Class Members entrusted Defendant with their Sensitive Information 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.

167. The injuries suffered by Plaintiffs 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 Plaintiffs and the Class Members' Sensitive Information.

168. 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.

169. 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 Plaintiffs and the Class Members. The policy of preventing future harm weighs in favor of finding a special relationship between Defendant and Plaintiffs and the Class. If companies are not held accountable for failing to take reasonable security measures to protect the Sensitive Information in their possession, they will not take the steps that are necessary to protect against future security breaches.

170. 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.

171. Defendant breached these duties through the conduct alleged in the Complaint by, including without limitation, failing to protect the Sensitive

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

172. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiffs and Class Members, their Sensitive Information 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 Sensitive Information of Plaintiffs and the Class Members were accessed by ill-intentioned criminals who could and will use the information to commit identity or financial fraud. Plaintiffs and Class Members face the imminent, certainly impending and substantially heightened risk of identity theft, fraud, and further misuse of their personal data.

173. 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 Sensitive Information in its possession or control would lead to one

or more types of injury to Plaintiffs and Class Members. And the Data Breach was foreseeable given the known, high frequency of cyberattacks and data breaches in the healthcare industry.

174. As a direct and proximate result of Defendant's negligence, Plaintiffs 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.

175. 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 Sensitive Information; illegal sale of the compromised Sensitive Information 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*
(On behalf of Plaintiffs and the Nationwide Class)

176. Plaintiffs incorporate paragraphs 1-160 of the Complaint as if fully set forth herein.

177. Plaintiffs and Class Members were required to provide non-public Sensitive Information in order to obtain medical services and prescription medications.

178. 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 Plaintiffs and Class Members.

179. 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.

180. 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 Plaintiffs' and Class Members' PII. *See* 15 U.S.C. § 1681(b).

181. Defendant solicited, gathered, and stored Sensitive Information of Plaintiffs and the Class Members to facilitate transactions which affect commerce.

182. Defendant violated the FTC Act (and similar state statutes), HIPAA, and the FCRA by failing to use reasonable measures to protect Sensitive Information of Plaintiffs 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 Sensitive Information obtained and stored and the foreseeable consequences of a data breach on Defendant's systems.

183. Defendant's violation of the FTC Act (and similar state statutes) as well as its violations of the FCRA constitutes negligence *per se*.

184. Plaintiffs and the Class Members are within the class of persons that the FTC Act (and similar state statutes) and the FCRA were intended to protect.

185. 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 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 Plaintiffs and the Class Members.

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

187. 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 Sensitive Information; illegal sale of the compromised Sensitive Information 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
Breach of Fiduciary Duty
(On Behalf of Plaintiffs and the Nationwide Class)

188. Plaintiffs incorporate paragraphs 1-160 of the Complaint as if fully set forth herein.

189. In providing their Sensitive Information to Defendant, Plaintiffs and Class Members justifiably placed a special confidence in Defendant to act in good

faith and with due regard to interests of Plaintiffs and Class Members to safeguard and keep confidential that Sensitive Information.

190. Defendant accepted the special confidence Plaintiffs and Class Members placed in it, as evidenced by its assertion that it is "committed to protecting the privacy of [Plaintiffs'] personal information" as included in the Data Breach notification letters.

191. In light of the special relationship between Defendant and Plaintiffs and Class Members, whereby Defendant became a guardian of Plaintiffs' and Class Members' Sensitive Information, Defendant became a fiduciary by its undertaking and guardianship of the Sensitive Information, to act primarily for the benefit of its customers, including Plaintiffs and Class Members for the safeguarding of Plaintiffs' and class member's Sensitive Information.

192. Defendant has a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of its customer's relationship, in particular, to keep secure the Sensitive Information of its customers.

193. Defendant breached its fiduciary duties to Plaintiffs and Class Members by failing to protect the integrity of the systems containing Plaintiffs' and Class Member's Sensitive Information.

194. Defendant breached its fiduciary duties to Plaintiffs and Class Members by otherwise failing to safeguard Plaintiffs' and Class Members' Sensitive Information.

195. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Sensitive Information; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Cyber-Attack and Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their Sensitive Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Sensitive Information in its continued possession; (vi) future costs in terms of time, effort, and money that will be expended as result of the Cyber-Attack and Data Breach for the remainder of the lives of Plaintiffs and class members; and (vii) the diminished value of Defendant's services they received.

196. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

197. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiffs are entitled to and demand actual, consequential, and nominal damages and injunctive relief.

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

198. Plaintiffs incorporate paragraphs 1-160 of the Complaint as if fully set forth herein.

199. Plaintiffs and other Class Members entered into valid and enforceable express contracts with Defendant under which Plaintiffs and other Class Members agreed to provide their Sensitive Information to Defendant, and Defendant agreed to provide testing services and, impliedly, if not explicitly, agreed to protect Plaintiffs and Class Members' Sensitive Information.

200. These contracts include HIPAA privacy notices and explanation of benefits documents.

201. To the extent Defendant's obligation to protect Plaintiffs' and other Class Members' Sensitive Information was not explicit in those express contracts,

the express contracts included implied terms requiring Defendant to implement data security adequate to safeguard and protect the confidentiality of Plaintiffs' and other Class Members' Sensitive Information, including in accordance with HIPAA regulations; federal, state and local laws; and industry standards. No Plaintiffs would have entered into these contracts with Defendant without understanding that Plaintiffs' and other class members' Sensitive Information would be safeguarded and protected.; Stated otherwise, data security was an essential implied term of the parties' express contracts.

202. A meeting of the minds occurred, as Plaintiffs and other class members agreed, among other things, to provide their Sensitive Information in exchange for Defendant's agreement to protect the confidentiality of that Sensitive Information.

203. The protection of Plaintiffs and Class Members' Sensitive Information were material aspects of Plaintiffs' and Class Members' contracts with Defendant.

204. Defendant's promises and representations described above relating to HIPAA and industry practices, and about Defendant' purported concern about their clients' privacy rights became terms of the contracts between Defendant and their clients, including Plaintiffs and other Class Members. Defendant breached these promises by failing to comply with HIPAA and reasonable industry practices.

205. Plaintiffs and Class Members read, reviewed, and/or relied on statements made by or provided by BioPlus and/or otherwise understood that BioPlus would protect its patients' Sensitive Information if that information were provided to BioPlus.

206. Plaintiffs and Class Members fully performed their obligations under the implied contract with Defendant; however, Defendant did not.

207. As a result of Defendant's breach of these terms, Plaintiffs and other Class Members have suffered a variety of damages including but not limited to: the lost value of their privacy; they did not get the benefit of their bargain with Defendant; they lost the difference in the value of the secure health services Defendant promised and the insecure services received; the value of the lost time and effort required to mitigate the actual and potential impact of the Data Breach on their lives, including, inter alia, that required to place "freezes" and "alerts" with credit reporting agencies, to contact financial institutions, to close or modify financial and medical accounts, to closely review and monitor credit reports and various accounts for unauthorized activity, and to file police reports; and Plaintiffs and other Class Members have been put at increased risk of future identity theft, fraud, and/or misuse of their Sensitive Information, which may take years to manifest, discover, and detect.

208. Plaintiffs and Class Members are therefore entitled to damages, including restitution and unjust enrichment, disgorgement, declaratory and injunctive relief, and attorney fees, costs, and expenses.

209. As a direct and proximate result of Defendant's breach of contract, Plaintiffs are entitled to and demand actual, consequential, and nominal damages and injunctive relief.

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

210. Plaintiffs incorporate paragraphs 1-160 of this Complaint as is fully restated herein.

211. This claim is brought in the alternative to Plaintiffs' claim for breach of express contract.

212. Through their course of conduct, Defendant, Plaintiff, and Class Members entered into implied contracts for the provision of healthcare services, as well as implied contracts for the Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiffs' and Class Members' Sensitive Information.

213. Specifically, Plaintiffs entered into a valid and enforceable implied contract with Defendant when she first entered into the testing services agreement with Defendant.

214. The valid and enforceable implied contract Class Members entered into with Defendant include Defendant's promise to protect nonpublic Sensitive Information given to Defendant or that Defendant creates on its own from disclosure.

215. When Plaintiffs and Class Members provided their Sensitive Information to Defendant in exchange for Defendant's services, they entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such information.

216. Defendant solicited and invited Class Members to provide their Sensitive Information as part of Defendant's regular business practices. Plaintiffs and Class Members accepted Defendant's offers and provided their Sensitive Information to Defendant.

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

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

219. Under implied contracts, Defendant and/or its affiliated providers promised and were obligated to: (a) provide pharmacy services to Plaintiffs and Class Members; and (b) protect Plaintiffs' and the Class Members' Sensitive Information provided to obtain such benefits of such services. In exchange, Plaintiffs and Members of the Class agreed to pay money for these services, and to turn over their Sensitive Information.

220. Both the provision of testing services and the protection of Plaintiffs' and Class Members' Sensitive Information were material aspects of these implied contracts.

221. The implied contracts for the provision of pharmacy services—contracts that include the contractual obligations to maintain the privacy of Plaintiffs' and Class Members' Sensitive Information—are also acknowledged, memorialized, and embodied in multiple documents, including (among other documents) Defendant's Data Breach notification letter.

222. Defendant's express representations, including, but not limited to the express representations found in its Privacy Notice, memorializes and embodies the implied contractual obligation requiring Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiffs and protect the privacy of Plaintiffs' and Class Members' Sensitive Information.

223. Consumers of pharmacy services value their privacy, the privacy of their dependents, and the ability to keep their Sensitive Information associated with obtaining such services. Plaintiffs and Class Members would not have entrusted their Sensitive Information to Defendant and entered into these implied contracts with Defendant without an understanding that their Sensitive Information would be safeguarded and protected, or entrusted their Sensitive Information to Defendant in the absence of its implied promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

224. A meeting of the minds occurred, as Plaintiffs and Class Members agreed and provided their Sensitive Information to Defendant and/or its affiliated healthcare providers, and paid for the provided testing services in exchange for, amongst other things, both the provision of healthcare and the protection of their Sensitive Information.

225. Plaintiffs and Class Members performed their obligations under the contract when they paid for Defendant's services and provided their Sensitive Information.

226. Defendant materially breached its contractual obligation to protect the nonpublic Sensitive Information Defendant gathered when the information was accessed and exfiltrated by the Data Breach.

227. Defendant materially breached the terms of the implied contracts, including, but not limited to, the terms stated in the relevant Notice of Privacy Practices. Defendant did not maintain the privacy of Plaintiffs' and Class Members Sensitive Information as evidenced by its notifications of the Data Breach to Plaintiffs and Class Members. Specifically, Defendant did not comply with industry standards, standards of conduct embodied in statutes like Section 5 of the FTCA, or otherwise protect Plaintiffs' and Class Members Sensitive Information as set forth above.

228. The Data Breach was a reasonably foreseeable consequence of Defendant's action in breach of these contracts.

229. As a result of Defendant's failure to fulfill the data security protections promised in these contracts, Plaintiffs and Class Members did not receive full benefit of the bargain, and instead received healthcare and other services that were of a diminished value to that described in the contracts. Plaintiffs and Class Members therefore were damaged in an amount at least equal to the difference in the value of the healthcare with data security protection they paid for and the healthcare they received.

230. Had Defendant disclosed that its security was inadequate or that it did not adhere to industry-standard security measures, neither the Plaintiff, Class

Members, nor any reasonable person would have purchased healthcare from Defendant and/or its affiliated providers.

231. As a direct and proximate result of the Data Breach, Plaintiffs and Class Members have been harmed and suffered, and will continue to suffer, actual damages and injuries, including without limitation the release and disclosure of their Sensitive Information, the loss of control of their Sensitive Information, the imminent risk of suffering additional damages in the future, disruption of their medical care and treatment, out of pocket expenses, and the loss of the benefit of the bargain they had struck with Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

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

233. As a direct and proximate result of Defendant's breach of contract, Plaintiffs are entitled to and demand actual, consequential, and nominal damages and injunctive relief.

COUNT VI
Violation of Florida's Deceptive and Unfair Trade Practices Act
Fla. Stat. § 501.201, *et seq.*
(On Behalf of Plaintiff David Gatz and the Florida Subclass)

234. Plaintiffs incorporate paragraphs 1-160 of the Complaint as if fully set forth herein.

235. Plaintiffs, Class Members, and Defendant each qualify as a person engaged in trade or commerce as contemplated by the Florida Deceptive and Unfair Trade Practices Act ("FDUTPA") Fla. Stat. § 501.201, *et seq.*

236. As alleged herein in this Complaint, Defendant engaged in unfair or deceptive acts or practices in the conduct of consumer transactions in violation of FDUTPA, including but not limited to:

a. Representing that its services were of a particular standard or quality that it knew or should have known were of another;

b. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs and Class Members' Sensitive Information, which was a direct and proximate cause of the Data Breach;

c. Failing to identify foreseeable security and privacy risks, and remediate identified security and privacy risks, which was a direct and proximate cause of the Data Breach;

d. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class Members' Sensitive Information, including duties imposed by the FTCA, 15 U.S.C. § 45, which was a direct and proximate cause of the Cyber-Attack and data breach;

e. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs' and Class Members' Sensitive Information, including by implementing and maintaining reasonable security measures;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Class Members' Sensitive Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class Members' Personal Information, including duties imposed by the FTCA, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach.

237. Defendant's representations and omissions were material because it was likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of consumers' Sensitive Information.

238. In addition, Defendant's failure to secure consumers' PHI violated the FTCA and therefore violated FDUTPA.

239. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard the Sensitive Information of Plaintiffs and Class Members, deter hackers, and detect a breach within a reasonable time, and that the risk of a data breach was highly likely.

240. The aforesaid conduct constitutes a violation of FDUTPA, Fla. Stat. § 501.204, in that it is a restraint on trade or commerce.

241. The Defendant's violations of FDUTPA have an impact of great and general importance on the public, including Floridians. Thousands of Floridians have used BioPlus Specialty Pharmacy's services, many of whom have been impacted by the Data Breach. In addition, Florida residents have a strong interest in regulating the conduct of its corporate citizens such as BioPlus, whose policies and practices described herein affected millions across the country.

242. As a direct and proximate result of Defendant's violation of FDUTPA, Plaintiffs and Class Members are entitled to a judgment under Fla. Stat. § 501.201, *et seq*, to enjoin further violations, to recover the costs of this action (including reasonable attorney's fees), and such other further relief as the Court deems just and proper.

243. Defendant's implied and express representations that it would adequately safeguard Plaintiffs' and other Class Members' Sensitive Information constitute representations as to characteristics, uses or benefits of services that such services did not actually have, in violation of Fla. Stat. § 501.202(2).

244. On information and belief, BioPlus formulated and conceived of the systems it used to compile and maintain patient information largely within the state of Florida, oversaw its data privacy program complained of herein from Florida, and its communications and other efforts to hold patient data largely emanated from Florida.

245. Most, if not all, of the alleged misrepresentations and omissions by BioPlus complained of herein that led to inadequate safety measures to protect patient information occurred within or were approved within Florida.

246. Defendant's implied and express representations that it would adequately safeguard Plaintiffs' and Class Members' Sensitive Information constitute representations as to the particular standard, quality, or grade of services that such services did not actually have (as the data security services were of another, inferior quality), in violation of Fla. Stat. § 501.204.

247. Defendant knowingly made false or misleading statements in its privacy policy regarding the use of personal information submitted by members of the public in that Defendant advertised it is committed to protecting privacy

and securely maintaining personal information. Defendant did not securely maintain personal information as represented, in violation of Fla. Stat. § 501.171.

248. These violations have caused financial injury to Plaintiff Gatz and Class Members and have created an unreasonable, imminent risk of future injury.

249. Accordingly, Plaintiff Gatz, on behalf of himself and the Florida Subclass, brings this action under the Deceptive and Unfair Trade Practices Act to seek such injunctive relief necessary to enjoin further violations and to recover costs of this action, including reasonable attorneys' fees and costs.

COUNT VII
Violation of New Jersey's Consumer Fraud Act
N.J. Rev. Stat. § 56:8-1, *et seq.*
(On Behalf of Plaintiff Wendy Bryan and New Jersey Subclass)

250. Plaintiffs incorporate paragraphs 1-160 of the Complaint as if fully set forth herein.

251. Plaintiffs, Class Members, and Defendant each qualify as a person engaged in trade or commerce as contemplated by New Jersey's Consumer Fraud Act, N.J. Rev. Stat. § 56:8-1, *et seq* ("CFA").

252. As alleged herein in this Complaint, Defendant engaged in unfair or deceptive acts or practices in the conduct of consumer transactions in violation of the CFA, including but not limited to:

a. Representing that its services were of a particular standard or quality that it knew or should have known were of another;

b. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs and Class Members' Sensitive Information, which was a direct and proximate cause of the Data Breach;

c. Failing to identify foreseeable security and privacy risks, and remediate identified security and privacy risks, which was a direct and proximate cause of the Data Breach;

d. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class Members' Sensitive Information, including duties imposed by the FTCA, 15 U.S.C. § 45, which was a direct and proximate cause of the Cyber-Attack and data breach;

e. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs' and Class Members' Sensitive Information, including by implementing and maintaining reasonable security measures;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Class Members' Sensitive Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the

security and privacy of Plaintiffs' and Class Members' Personal Information, including duties imposed by the FTCA, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach.

253. Defendant's representations and omissions were material because it was likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of consumers' Sensitive Information.

254. In addition, Defendant's failure to secure consumers' PHI violated the FTCA and therefore violates the CFA.

255. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard the Sensitive Information of Plaintiffs and Class Members, deter hackers, and detect a breach within a reasonable time, and that the risk of a data breach was highly likely.

256. The aforesaid conduct constitutes a violation of the CFA, in that it is a restraint on trade or commerce.

257. The Defendant's violations of the CFA have an impact of great and general importance on the public, including New Jerseyans. Thousands of New Jerseyans have used BioPlus Specialty Pharmacy's services, many of whom have been impacted by the Data Breach. In addition, New Jersey residents have a strong interest in regulating the conduct of corporations that do business within the

state's such as BioPlus, whose policies and practices described herein affected millions across the country.

258. As a direct and proximate result of Defendant's violation of the CFA, Plaintiffs and Class Members are entitled to a judgment under N.J. Rev. Stat. § 56:8-1, *et seq*, to enjoin further violations, to recover actual damages, to recover the costs of this action (including reasonable attorney's fees), and such other further relief as the Court deems just and proper.

259. Defendant's implied and express representations that it would adequately safeguard Plaintiffs' and other Class Members' Sensitive Information constitute representations as to characteristics, uses or benefits of services that such services did not actually have, in violation of the CFA.

260. Defendant's implied and express representations that it would adequately safeguard Plaintiffs' and Class Members' Sensitive Information constitute representations as to the particular standard, quality, or grade of services that such services did not actually have (as the data security services were of another, inferior quality), in violation of the CFA.

261. Defendant knowingly made false or misleading statements in its privacy policy regarding the use of personal information submitted by members of the public in that Defendant advertised it is committed to protecting privacy and securely maintaining personal information. Defendant did not securely

maintain personal information as represented, in violation of the CFA. N.J. Rev. Stat. § 56:8-196.

262. Further, BioPlus inexplicably waited nearly one month before it began sending notification letters to customers of the data breach incident. This delay resulted in additional harms to customers who were not notified that their data was lost until over 30 days after the incident, leaving the information exposed and vulnerable to misuse without customers' knowledge, a violation of N.J. Rev. Stat. § 56:8-163.

263. These violations have caused financial injury to Plaintiffs and Class Members and have created an unreasonable, imminent risk of future injury.

264. Accordingly, Plaintiffs, on behalf of themselves and the other Class Members, bring this action under the Consumer Fraud Act to seek such injunctive relief necessary to enjoin further violations and to recover costs of this action, including reasonable attorneys' fees and costs.

COUNT VIII
Violation of the Connecticut Unfair Trade Practices Act
Con. Gen, Stat. §42-110, *et seq.*
(On Behalf of Plaintiff Patricia White and Connecticut Subclass)

265. Plaintiffs incorporate paragraphs 1-160 of the Complaint as if fully set forth herein.

266. Plaintiffs, Class Members, and Defendant each qualify as a person engaged in trade or commerce as contemplated by the Connecticut Unfair Trade Practices Act. Con. Gen, Stat. §42-110(a) ("CUTPA").

267. As alleged herein in this Complaint, Defendant engaged in unfair or deceptive acts or practices in the conduct of consumer transactions in violation of the CUTPA, including but not limited to:

a. Representing that its services were of a particular standard or quality that it knew or should have known were of another;

b. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Class Members' Sensitive Information, which was a direct and proximate cause of the Data Breach;

c. Failing to identify foreseeable security and privacy risks, and remediate identified security and privacy risks, which was a direct and proximate cause of the Data Breach;

d. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class Members Sensitive Information, including duties imposed by the FTCA, 15 U.S.C. § 45, which was a direct and proximate cause of the Cyber-Attack and data breach;

e. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs' and Class Members' Sensitive Information, including by implementing and maintaining reasonable security measures;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Class Members' Sensitive Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class Members' Personal Information, including duties imposed by the FTCA, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach.

268. Defendant's representations and omissions were material because it was likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of consumers' Sensitive Information.

269. In addition, Defendant's failure to secure consumers' PHI violated the FTCA and therefore violates the CUTPA.

270. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard the Sensitive Information

of Plaintiffs and Class Members, deter hackers, and detect a breach within a reasonable time, and that the risk of a data breach was highly likely.

271. The aforesaid conduct constitutes a violation of the CUTPA, Con. Gen, Stat. §42-110 *et seq.*, in that it is a restraint on trade or commerce.

272. The Defendant's violations of the CUTPA have an impact of great and general importance on the public, including people from Connecticut. Thousands of Connecticut citizens have used BioPlus's services, many of whom have been impacted by the Data Breach. In addition, Connecticut residents have a strong interest in regulating the conduct of its corporate citizens such as BioPlus, whose policies and practices described herein affected millions across the country.

273. As a direct and proximate result of Defendant's violation of the CUTPA, Plaintiffs and Class Members are entitled to a judgment under Con. Gen, Stat. §42-110 *et seq.*, to enjoin further violations, to recover actual damages, to recover the costs of this action (including reasonable attorney's fees), and such other further relief as the Court deems just and proper.

274. Defendant's implied and express representations that it would adequately safeguard Plaintiffs' and other Class Members' Sensitive Information constitute representations as to characteristics, uses or benefits of services that such services did not actually have, in violation of Con. Gen, Stat. §42-110(a).

275. Defendant's implied and express representations that it would adequately safeguard Plaintiffs' and Class Members' Sensitive Information constitute representations as to the particular standard, quality, or grade of services that such services did not actually have (as the data security services were of another, inferior quality), in violation of Con. Gen, Stat. §42-110(a).

276. Defendant knowingly made false or misleading statements in its privacy policy regarding the use of personal information submitted by members of the public in that Defendant advertised it is committed to protecting privacy and securely maintaining personal information. Defendant did not securely maintain personal information as represented, in violation of Con. Gen, Stat. §42-110(a).

277. These violations have caused financial injury to Plaintiffs and Class Members and have created an unreasonable, imminent risk of future injury.

278. Accordingly, Plaintiffs, on behalf of themselves and the other Class Members, bring this action under the CUTPA to seek such injunctive relief necessary to enjoin further violations and to recover costs of this action, including reasonable attorneys' fees and costs.

COUNT IX
Violation of O.C.G.A. § 13-6-11
(On behalf of Plaintiff Gilbert and the Georgia subclass)

279. Plaintiffs incorporate paragraphs 1-160 of the Complaint as if fully set forth herein.

280. Defendant through its actions alleged and described herein acted in bad faith, was stubbornly litigious, or caused Plaintiffs unnecessary trouble and expense with respect to the transaction or events underlying this litigation.

281. 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 companies such as Defendant for failing to implement and use reasonable measures to protect PII. Various FTC publications and orders also form the basis of Defendant's duty.

282. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect personal and sensitive data and not complying with the industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of personal and sensitive data it obtained and stored and the foreseeable consequences of a data breach.

283. Defendant also has a duty under the Georgia Constitution ('the Constitution') which contains a Right to Privacy clause, Chapter 1, Article 1, to protect its users' private information. The Georgia Constitution states, "no person shall be deprived of life, liberty, or property except by due process of law." Moreover, the Georgia Constitution identifies certain invasions of privacy,

including the Public Disclosure of Private Life which prohibits the public disclosure of private facts.

284. This duty has been recognized by the Georgia Supreme Court in the Restatement of the Law of Torts (Second) §652A which specifically recognized four common law invasion of privacy claims in Georgia, which include: 1) appropriation of likeness; 2) intrusion on solitude or seclusion; 3) public disclosure of private facts; and 4) false light.

285. Defendant's implementation of inadequate data security measures, its failure to resolve known vulnerabilities and deficiencies, and its abdication of its responsibility to reasonably protect data it required users to provide and stored on its own servers and databases constitutes a violation of the Georgia Constitution and the Restatement of the Law of Torts (Second).

286. Defendant knew or should have known that it had a responsibility to protect the consumer data it required users to provide and stored, that it was entrusted with this data, and that it was the only entity capable of adequately protecting the data on its systems and databases.

287. Despite that knowledge, Defendant abdicated its duty to protect the data it solicited and stored, and instead put the onus on its users to protect their data. For example, Defendant represented to users that the only real risk of the theft of their data came from the users themselves, and the theft of data off of

their smart phones, not supposedly "numerous methods by which hackers may steal information from [users'] computers and hand-held devices." Indeed, Defendant flatly represented that its practices were not "100% secure" and that it would "not guarantee the security of your information." Thus, despite collecting and storing users' personal and sensitive data, Defendant did not intend to protect it. Rather, it hoped to avoid any responsibility and liability for stolen data by claiming it was impossible to fully protect it.

288. That, however, is not true. As numerous data security experts and data security standards make clear, even bare minimum measures can protect stored data from a data breach. Defendant, however, refused to do the bare minimum. Indeed, it wasn't until after the Data Breach that Defendant took efforts to improve its data security and remove vulnerabilities that existed within its digital platforms.

289. Unfortunately for Plaintiffs and the Class, Defendant's efforts came too late. As a direct and proximate result of Defendant's actions, Plaintiffs' and the Class's personal and sensitive data was stolen, put up for sale on the Dark Web, and eventually, posted in plain view on a Dark Web forum for anyone to view and steal. As further alleged above, the Data Breach was a direct consequence of Defendant's abrogation of data security responsibility and its decision to employ knowingly deficient data security measures that knowingly left the

personal and sensitive data unsecured. Had Defendant adopted reasonable data security measures, it could have prevented the Data Breach.

290. As further described above, Plaintiffs and the Class have been injured and suffered losses directly attributable to the Data Breach.

291. Plaintiffs therefore request that their claim for recovery of expenses of litigation and attorneys' fees be submitted to the jury, and that the Court enter a Judgment awarding their expenses of litigation and attorneys' fees pursuant to O.C.G.A. § 13-6-11.

COUNT X
North Carolina Deceptive Trade Practices Act, N.C. Gen. Stat. § 75-1.1, *et seq.*
(On behalf of Plaintiffs Crystal Hullet, Alicia Dunn, and the North Carolina Subclass)

292. Plaintiffs incorporate paragraphs 1-160 of the Complaint as if fully set forth herein.

293. North Carolina law declares unlawful all "unfair or deceptive acts or practices in or affecting commerce" N.C. Gen. Stat. § 75-1.1.

294. "Commerce" is defined broadly as any business activity other than "professional services rendered by a members of a learned profession." *Id.*

295. Defendant engaged in unlawful, unfair, and deceptive acts and practices, misrepresentations, and the concealment, suppression, and omission of material facts with respect to the sale and advertisement of the services used by

Plaintiffs and the North Carolina Subclass in violation of N.C. Gen. Stat. § 75-1.1, including but not limited to the following:

a. Defendant omitted, suppressed, and concealed the material fact of the inadequacy of the privacy and security protections for the North Carolina Subclass's Sensitive Information;

b. Defendant engaged in unfair, unlawful, and deceptive acts and practices with respect to its loan services by failing to maintain the privacy and security of the North Carolina Subclass's Sensitive Information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the Data Breach. These unfair, unlawful, and deceptive acts and practices violated duties imposed by laws including the FTC Act, 15 U.S.C. § 45 and HIPAA, 42 U.S.C. § 1302d, *et seq.*;

c. Defendant engaged in unlawful, unfair, and deceptive acts and practices with respect to its loan services by failing to disclose the Data Breach to the North Carolina Subclass in a timely and accurate manner; and

d. Defendant engaged in unlawful, unfair, and deceptive acts and practices with respect to its loans services by failing to take proper action following the Data Breach to enact adequate privacy and

security measures and protect the North Carolina Subclass's Sensitive Information from further unauthorized disclosure, release, data breach, and theft.

296. The above unlawful, unfair, and deceptive acts and practices by Defendant were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to consumers that the consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

297. Defendant knew or should have known that its computer systems, email accounts, and data security practices were inadequate to safeguard the North Carolina Subclass's Sensitive Information and that risk of a data breach or theft was highly likely. Defendant's actions in engaging in the above-named deceptive acts and practices were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the North Carolina Subclass.

298. As a direct and proximate result of Defendant's deceptive acts and practices, the North Carolina Subclass members suffered an ascertainable loss, as described above, including the loss of their legally protected interest in the confidentiality and privacy of their Sensitive Information.

299. Individuals injured by unfair or deceptive acts or practices are entitled to treble damages. N.C. Gen. Stat. § 75-16. 238. Plaintiffs and the North

Carolina Subclass seek relief under N.C. Gen. Stat. §§ 75-1.1, *et seq.*, and request treble damages, attorney fees, expenses, and costs, and injunctive relief.

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

300. Plaintiffs incorporate paragraphs 1-160 of the Complaint as if fully set forth herein.

301. 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.

302. 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' Sensitive Information, and whether Defendant is currently maintaining data security measures adequate to protect Plaintiffs and Class Members from further data breaches that compromise their Sensitive Information. Plaintiffs and Class Members remain at imminent risk that further compromises of their Sensitive Information will occur in the future. This is true even if they (or their healthcare providers) are not actively using Defendant's products or services.

303. 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' Sensitive Information 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' Sensitive Information.

304. 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' Sensitive Information.

305. 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. 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.

306. The hardship to 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 to Defendant, 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 a pre-existing legal obligation to employ such measures.

307. 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 to Defendant, thus eliminating additional injuries that would result to Plaintiff, Class Members, and the millions of other Defendant customers whose Sensitive Information 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 Subclasses, 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 Sensitive Information 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 Sensitive Information of

Plaintiffs and Class Members;

v. prohibiting Defendant from maintaining the Sensitive Information 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.

JURY TRIAL DEMANDED

Pursuant to Federal Rule of Civil Procedure 38(b), Plaintiffs demand 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*)
Dylan J. Gould (*Pro Hac Vice* Forthcoming)
MARKOVITS, STOCK & DEMARCO, LLC
119 East Court Street, Suite 530
Cincinnati, OH 45202
Phone: (513) 651-3700
tcoates@msdlegal.com
dgould@msdlegal.com

Scott David Hirsch
SCOTT HIRSCH LAW GROUP PLLC
Fla. Bar No. 50833
6810 N. State Road 7
Coconut Creek, FL 33073
Phone: (561) 569-7062
scott@scotthirschlawgroup.com

Nicholas A. Migliaccio (*Pro Hac Vice*)
Jason S. Rathod (*Pro Hac Vice*)
MIGLIACCIO & RATHOD LLP
412 H Street NE
Washington, DC 20002
Tel: (202) 470-3520
nmigliaccio@classlawdc.com
jrathod@classlawdc.com

Joseph M. Lyon (*Pro Hac Vice*)
THE LYON FIRM, LLC
2754 Erie Avenue
Cincinnati, OH 45208
Phone: (513) 381-2333
jlyon@thelyonfirm.com

Avi R. Kaufman
KAUFMAN P.A.
237 S. Dixie Hwy., 4th Flr.
Coral Gables, FL 33133
Phone: (305) 469-5881
kaufman@kaufmanpa.com

Lynn A. Toops
COHEN & MALAD LLP
One Indiana Square, Suite 1400
Indianapolis, IN 46204
Phone: (317) 636-6481
ltoops@cohenandmalad.com

J. Gerard Stranch, IV
Peter J. Jannace
BRANSTETTER STRANCH & JENNINGS PLLC
223 Rosa L. Parks Avenue, Suite 200
Nashville, TN 37203
Phone: (615) 354-8801
gerards@bsjfirm.com
peter@bsjfirm.com

Gary Mason (*Pro Hac Vice* Forthcoming)
MASON LLP
5301 Wisconsin Avenue, NW. Suite 305 Washington, DC 20016 Phone: (202) 429-2290
gmason@masonllp.com

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

Katherine Earle Yanes
KYNES, MARKMAN & FELMAN, P.A.
P.O. Box 3396
Tampa, FL 33601
Phone: (813) 229-1118
kyanes@kmf-law.com

Counsel for Plaintiffs and the Class

CERTIFICATE OF SERVICE

I hereby certify that on March 28, 2022, I electronically filed the foregoing document with the Clerk of Court by using the Florida E-Filing Portal, which will send a Notice of Electronic Filing to all counsel of record.

/s/ John A. Yanchunis
John A. Yanchunis