UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF FLORIDA
ORLANDO DIVISION

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

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

NATURE OF THE ACTION

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

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

DOCKET ALARM
Find authenticated court documents without watermarks at docketalarm.com.

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

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

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

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

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

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

DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.

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

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

10. Plaintiff and Class Members relied on Defendant to keep their PII and PHI confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

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

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

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

DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.

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

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

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

THE PARTIES

Plaintiff Bonnie Gilbert

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

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

DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.

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

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

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

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

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

Defendant BioPlus

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

24. BioPlus advertises itself as its patients' "24/7 partner in health." It helps provides medications and individual therapeutic care plans to help patients manage conditions like hepatitis,

DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.