IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

LAURA HERNANDEZ, Individually and on Behalf of All Others Similarly Situated, Plaintiff, v. WALGREEN COMPANY, Defendant.	)	Case No.: **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Laura Hernandez ("Plaintiff"), individually, by and through her undersigned counsel, brings this class action lawsuit against Walgreen Company ("Defendant," or "Walgreens"), on behalf of herself and all others similarly situated, and alleges, based upon information and belief and the investigation of her counsel as follows:

INTRODUCTION

1. Walgreens is the second-largest pharmacy store chain in the United States specializing in prescription fulfillment, health and wellness products, health information, and photo services. As of mid-2019, the company operated 9,277 stores across 50 states.

2. On or about September 26, 2019, Walgreens discovered abnormal activity on a number of Walgreens.com customer accounts wherein purportedly valid login information was used to gain illegal access to such accounts. With those credentials, unauthorized third parties gained

access to the sensitive personally identifiable information ("PII and PHI") and protected health information ("PHI") of Walgreens customers.[1]

3. The exposed PII and PHI included: one or more drug classifications that were derived from customer prescription record histories (e.g. beta blockers, calcium channel blockers, antihypertensives); one or more health-related suggestions referencing an assumed health condition or health-related topic (e.g.. asthma, COPD, migraines, blood pressure maintenance); demographic information including first name, last name, date of birth, phone number, and/or email address; Walgreens Balance Rewards ID and/or Balance Rewards Card Number; and AARP ID Numbers. (the "Data Breach").

4. While Walgreens discovered that its system had been compromised or about September 26, 2019, and identified affected customers by October 5, 2019, it failed to provide notice of the Data Breach until December 3, 2019.

5. This Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect customer PII and PHI.

[1] Personally identifiable information generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual. PII AND PHI also is generally defined to include certain identifiers that do not on their face name an individual, but that are considered to be particularly sensitive and/or valuable if in the wrong hands (for example, Social Security number, passport number, driver's license number, financial account number). Under HIPAA, protected health information ("PHI") is considered to be individually identifiable information relating to the past, present, or future health status of an individual that is created, collected, or transmitted, or maintained by a HIPAA-covered entity in relation to the provision of healthcare, payment for healthcare services, or use in healthcare operations. 45 C.F.R. § 160.103. Health information such as diagnoses, treatment information, medical test results, and prescription information are considered protected health information under HIPAA, as are national identification numbers and demographic information such as birth dates, gender, ethnicity, and contact and emergency contact information. https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html.

6. Defendant disregarded the rights of Plaintiff and Class Members (defined below) by, *inter alia*, intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions; failing to disclose that it did not have adequately robust computer systems and security practices to safeguard patient PII and PHI; failing to take standard and reasonably available steps to prevent the Data Breach; and failing to provide Plaintiff and Class Members prompt and accurate notice of the Data Breach.

7. As a result of Defendant's failure to implement and follow basic security procedures, patient PII and PHI is now in the hands of thieves. Plaintiff and Class Members have had to spend, and will continue to spend, significant amounts of time and money in an effort to protect themselves from the adverse ramifications of the Data Breach, and will forever be at a heightened risk of identity theft and fraud.

8. Plaintiff, on behalf of all others similarly situated, alleges claims for negligence, invasion of privacy, breach of implied contract, unjust enrichment, breach of fiduciary duty, and violation of the Florida Unfair Deceptive Trade Practices Act and seeks to compel Defendant to adopt reasonably sufficient security practices to safeguard patient PII and PHI that remains in its custody in order to prevent incidents like the Data Breach from reoccurring in the future.

PARTIES

9. Plaintiff Laura Hernandez is a resident of Oakland Park, Florida and a Walgreens customer. On or about December 3, 2019, Ms. Hernandez received notice from Walgreens that her sensitive PII and PHI had been improperly exposed to unauthorized third parties.

10. Upon receiving notice of the Data Beach, Ms. Hernandez has undertaken the following actions: (a) changed her on-line credentials; (b) changed her security question; (c)

conducted research regarding password management tools; (d) changed her credentials and login details in at least 7 different websites where she used the same login details; (e) checked her health insurance activity online and made 5 phone calls to her health insurance company (lasting over an hour each time, plus waiting time) to ensure that personal information and claims during 2018 and 2019 were correct and no unauthorized claims had been made; (f) contacted her financial institution telephonically on multiple occasions to inform it of the breach and request that her account be monitored for any unusual activity; (g) checked bank activity and changed credentials to ensure no unauthorized purchases were made; (h) checked her credit account to review all activity and credit score information reported during 2018 and 2019, and changed credentials; (i) requested credit reports from all three major credit bureaus to review all activity and credit score information during 2018 and 2019 in order to ensure no unauthorized activity; (j) contacted all medical providers from 2018 and 2019 and requested medical records, prescriptions and history during 2018 & 2019 to ensure information was correct and no unauthorized claims had been made.

11. To support these actions, Ms. Hernandez spent time doing the following: (a) determining through research and email history the identity of her medical providers over the past two years including pharmacies, primary care physicians and specialists; (b) contacting each provider personally by driving to each facility, taking time off work; (c) preparing personalized letters to each provider requesting medical records during 2018 and 2019; (d) following up over email and phone with each provider until confirmation was received that the medical records were ready; (e) reviewing all her account statements, prescription histories and medical records.

12. In addition to the time spent, Ms. Hernandez also had to pay for gasoline to drive to each medical facility and copying costs.

13. Since the announcement of the Data Breach, Ms. Hernandez continues to monitor her accounts in an effort to detect and prevent any misuse of her personal information.

14. Ms. Hernandez has, and continues to spend her valuable time to protect the integrity of her PII and PHI—time which she would not have had to expend but for the Data Breach.

15. Plaintiff suffered actual injury from having her PII and PHI stolen as a result of the Data Breach including, but not limited to: (a) paying monies to Walgreens for its goods and services which she would not have had if Walgreens disclosed that it lacked data security practices sufficient to safeguard consumers' PII and PHI from theft; (b) damages to and diminution in the value of her PII and PHI—a form of intangible property that the Plaintiff entrusted to Walgreens as a condition for health related services; (c) loss of her privacy; (d) imminent and impending injury arising from the increased risk of fraud and identity theft.

16. As a result of the Data Breach, Ms. Hernandez will continue to be at heightened risk for financial fraud, medical fraud and identity theft, and their attendant damages for years to come.

17. Defendant Walgreen Company is headquartered at 200 Wilmot Road Deerfield, IL 60015. It is the second largest pharmacy store chain in the United States specializing prescription fulfillment, health and wellness products, health information, and photo services. As of mid-2019, the company operated 9,277 stores across 50 states.

JURISDICTION AND VENUE

18. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. While the exact number of putative class members is unknown, upon

information and belief, they number in the thousands. At least some of the putative class members have a different citizenship from Walgreens.

19. This Court has jurisdiction over the Defendant which operates in this District, and the computer systems implicated in this Data Breach are likely based in this District.

20. Plaintiff received services from Walgreens and engaged in underlying health services within this District. Through its business operations in this District, Walgreens intentionally avails itself of the markets within this District to render the exercise of jurisdiction by this Court just and proper.

21. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events and omissions giving rise to this action occurred in this District. Walgreens is based in this District, maintains patient PII and PHI in the District, and has caused harm to Plaintiff and Class members residing in this District.

STATEMENT OF FACTS

A. The Walgreens Data Breach

22. On or about September 26, 2019, Walgreens discovered abnormal activity on a number of Walgreens.com customer accounts wherein valid logins were used to gain illegal access to such accounts. With those credentials, unauthorized users gained access to the sensitive personally identifiable information and protected health information of Walgreens' customers.

23. On December 3, 2019, Walgreens notified affected customers of the Data Breach stating in relevant part as follows:

> We recently learned of unauthorized access associated with and limited to your Walgreens,com account ("Account"). We are contacting you to provide you with information about the incident and also with information about steps you can take to protect yourself.

WHAT HAPPENED

On or about September 26, 2019, Walgreens discovered seemingly abnormal activity for a limited number of Walgreens.com customer accounts. Our investigation indicates that this abnormal activity was the result of valid login credentials obtained from non-Walgreens sites and used to gain access to your Walgreens Account. Walgreens promptly took steps to address the unauthorized access upon learning of the incident by engaging an industry leader in cybersecurity to assist in the investigation, as well as implementing enhanced security protections. In addition, we implemented forced locks on the impacted accounts to further protect you.

On or about October 5, 2019, Walgreens determined that limited health-related information may have been viewed or accessed for a small percentage of impacted customers. We have determined that you were part of the impacted customer group and that your limited health-related information, as further described below, may have been accessed in your Account between September 10 and September 28, 2019.

WHAT INFORMATION WAS INVOLVED

It appears that the following types of information were subject to unauthorized access, in a manner that could have been associated with your Account:

- One or more drug classifications associated with you that were derived from your prescription record history (e.g. beta blockers, calcium channel blockers. antihypertensives);

- One or more health-related suggestions referencing an assumed health condition or health-related topic (e.g.. asthma. COPD, migraines, blood pressure maintenance);

- Demographic information that may have included your first name, last name, date of birth, phone number, and/or email address;

- Your Walgreens Balance Rewards ID and/or Balance Rewards Card Number if you are enrolled in Balance Rewards; and

- Your AARP ID Number if you linked it to your Walgreens Account

WHAT ARE WE DOING

Walgreens implemented enhanced security protections and initiated Walgreens.com and mobile account locks on potentially impacted accounts, forcing password resets. Walgreens has also engaged the professional services of an industry leader in cybersecurity. Based on expert guidance, we believe the unauthorized access is consistent with patterns seen in the retail industry in similar events to be focused on theft of loyalty account points. For Walgreens, this is our Balance Rewards Program.

WHAT YOU CAN DO

As detailed above, Walgreens promptly took affirmative steps to lock your Account, which requires you to select a new password. When you reset your password, we urge you, for your protection, to use login credentials unique to your Walgrcens.com account going forward. For enhanced password effectiveness, consider using strong passwords. If you used your existing Walgreens.com account password as the password on any other websites, we also encourage you to change your password on those websites as well. In addition to resetting your password, we encourage you to promptly change your Account security question and take the same action with other online accounts where the same username or email address and password are used. Further, we recommend that you evaluate whether you should use password management tools for enhanced online security.

Additionally, Walgreens urges customers to remain vigilant by reviewing account statements and monitoring free credit reports as a precaution. We also recommend that customers monitor their prescription and medical records. We have enclosed information on steps you can take to further protect your information, and how to obtain a free copy of your credit report from each of the three (3) major credit reporting agencies.

FOR MORE INFORMATION

For further information and assistance, or if you identify any unauthorized use of your Wallgreens.com account or Balance Rewards information, as applicable, please contact Walgreens' toll free number at (877) 924-4472. You can also contact us in writing at 200 Wilmot Road, MS 9000, Deerfield, Illinois 60015.[2]

[2] Walgreens, Notice of Data Breach, December 3, 2019 attached hereto as Exhibit A.

B. Walgreens' Privacy Policies

24. Walgreens maintains detailed privacy policies and practices wherein it recognizes that it collects customer PII and PHI and has a commensurate duty to "maintain the privacy" of such PII and PHI.[3] Walgreens assures its customers the following:

> You trust us with your health and wellness needs, and we take that responsibility seriously. That includes making sure your data is safe and secure, and that you have control.
>
> We are committed to maintaining our customers' privacy. We take great care to safeguard the information that we collect to maintain our customers' privacy.
>
> Walgreens recognizes the importance of maintaining the security of your information. Whether you are shopping on our website, through our mobile services, or in our stores, we use reasonable security measures, including administrative, technical, and physical safeguards.[4]

25. Despite these assurances, as evidenced by the Data Breach, Walgreens has failed to live up to its commitments and obligations to protect patient PII and PHI.

C. Prevalence of Cyber Attacks and Particular Susceptibility of the Healthcare Sector

26. In 2016, the number of U.S. data breaches surpassed 1,000, a record high and a forty percent increase in the number of data breaches from the previous year.[5] In 2017, a new record high of 1,579 breaches were reported, representing a 44.7 percent increase over 2016.[6]

---

[3] Notice of Privacy Practices, https://www.walgreens.com/topic/help/general/noticeprivacypractices.jsp?foot=privacy

[4] Online Privacy and Security Policy, https://www.walgreens.com/topic/help/generalhelp/privacyandsecurity.jsp

[5] Identity Theft Resource Center, *Data Breaches Increase 40 Percent in 2016, Finds New Report From Identity Theft Resource Center and CyberScout* (Jan. 19, 2017), *available at* https://www.idtheftcenter.org/surveys-studys.

[6] Identity Theft Resource Center, 2017 Annual Data Breach Year-End Review, available at https://www.idtheftcenter.org/2017-data-breaches/.

27. In 2018, the healthcare sector reported the second largest number of breaches among all measured sectors and the highest rate of exposure per breach.[7] Indeed, healthcare related data is among the most sensitive, and personally consequential when compromised. A report focusing on health-care breaches found that the "average total cost to resolve an identity theft-related incident…came to about $20,000," and that the victims were often forced to pay out-of-pocket costs for health care they did not receive in order to restore coverage.[8] Almost 50 percent of the victims lost their health care coverage as a result of the incident, while nearly one-third said their insurance premiums went up after the event. Forty percent of the customers were never able to resolve their identity theft at all. Data breaches and identity theft have a crippling effect on individuals and detrimentally impact the entire economy as a whole.[9]

28. Healthcare related data breaches, in particular, have continued to rapidly increase. According to the 2019 HIMSS Cybersecurity Survey, 82 percent of participating hospital information security leaders reported having a significant security incident in the last 12 months, with a majority of these known incidents being caused by "bad actors" such as cybercriminals.[10]

29. As a healthcare provider Walgreens knew, or should have known, the importance of safeguarding patient PII and PHI entrusted to it and of the foreseeable consequences if its data security systems were breached, including the significant costs that would be imposed on its patients as a result of a breach, yet failed to take adequate cyber-security measures to prevent the Data Breach from occurring.

---

[7] Identity Theft Resource Center, 2018 End -of-Year Data Breach Report. Available at https://www.idtheftcenter.org/2018-data-breaches/.
[8] Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (March 3, 2010) https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/.
[9] *Id.*
[10] https://www.himss.org/2019-himss-cybersecurity-survey (last visited June 14, 2019).

D. Walgreens Acquires, Collects, and Stores Plaintiff's and Class Members' PII and PHI

30. Walgreens acquires, collects, and stores a massive amount of protected health related information and other personally identifiable data on its customers.

31. As a condition of engaging in health services, Walgreens requires that these patients entrust them with highly sensitive personal information.

32. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PII and PHI, Walgreens assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' PII and PHI from disclosure.

33. Plaintiff and the Class Members have taken reasonable steps to maintain the confidentiality of their PII and PHI. Plaintiff and the Class Members, as current and former patients, relied on Walgreens 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.

E. The Value of Personally Identifiable Information and the Effects of Unauthorized Disclosure

34. Walgreens was well-aware that the PII and PHI it collects is highly sensitive and of significant value to those who would use it for wrongful purposes.

35. Personally identifiable information is a valuable commodity to identity thieves. As the FTC recognizes, with PII and PHI identity thieves can commit an array of crimes including identify theft, medical and financial fraud.[11] Indeed, a robust "cyber black market"

[11] Federal Trade Commission, *Warning Signs of Identity Theft*, https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft

exists in which criminals openly post stolen PII and PHI on multiple underground Internet websites.

36. While credit card information and associated PII can sell for as little as $1 to $2 on the black market, protected health information can sell for as much as $363 according to the Infosec Institute. This is because one's personal health history (e.g. ailments, diagnosis, surgeries, etc.) cannot be changed.[12] The combination of PII and PHI is particularly valuable because criminals can use it to target victims with frauds and scams that take advantage of the victim's medical conditions or victim settlements. It can be used to create fake insurance claims, allowing for the purchase and resale of medical equipment, or gain access to prescriptions for illegal use or resale.

37. The ramifications of Walgreens' failure to keep its patients' PII and PHI secure are long lasting and severe. Once PII and PHI is stolen, fraudulent use of that information and damage to victims may continue for years.

38. At all relevant times, Walgreens knew, or reasonably should have known, of the importance of safeguarding PII and PHI and of the foreseeable consequences if its data security systems were breached, including, the significant costs that would be imposed on patients as a result of a breach.

F. Walgreens' Conduct Violates HIPAA

39. HIPAA requires covered entities to protect against reasonably anticipated threats to the security of PHI. Covered entities must implement safeguards to ensure the confidentiality,

[12] Center for Internet Security, Data Breaches: In the Healthcare Sector, https://www.cisecurity.org/blog/data-breaches-in-the-healthcare-sector/

integrity, and availability of PHI. Safeguards must include physical, technical, and administrative components.[13]

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

41. Defendant's Breach resulted from a combination of insufficiencies that demonstrate Defendant failed to comply with safeguards mandated by HIPAA regulations. Walgreens' security failures include, but are not limited to:

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

b. Failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. §164.312(a)(1);

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

d. Failing to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents

[13] https://www.hipaajournal.com/what-is-considered-protected-health-information-under-hipaa/

that are known to the covered entity in violation of 45 C.F.R. §164.308(a)(6)(ii);

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

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

g. Failing to ensure compliance with HIPAA security standard rules by its workforce in violation of 45 C.F.R. §164.306(a)(94);

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

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

j. Failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably

safeguard protected health information, in compliance with 45 C.F.R. §164.530(c).

G. Walgreens Fails to Comply with FTC Guidelines

42. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[14]

43. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses.[15] The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.

44. The FTC further recommends that companies not maintain PII AND PHI longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[16]

45. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and

---

[14] Federal Trade Commission, *Start With Security*, available at https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

[15] Federal Trade Commission, *Protecting Personal Information: A Guide for Business*, available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

[16] FTC, *Start With Security*, *supra* note 19.

appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

46. Walgreens failed to properly implement basic data security practices. Walgreens' failure to employ reasonable and appropriate measures to protect against unauthorized access to patient PII AND PHI constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

47. Walgreens was at all times fully aware of its obligation to protect the PII AND PHI of patients because of its position as a trusted healthcare provider. Walgreens was also aware of the significant repercussions that would result from its failure to do so.

H. Walgreens Fails to Comply with Industry Standards

48. Data exfiltrated from healthcare providers continues to be a high value target among cybercriminals. In 2017, the U.S. healthcare sector experienced over 330 data breaches, a number which continued to grow in 2018 (363 breaches).[17] The costs of healthcare data breaches are among the highest across all industries, topping $380 per stolen record in 2017 as compared to the global average of $141 per record. *Id.* As a result, both the government and private sector have developed industry best standards to address this growing problem.

49. The Department of Health and Human Services' Office for Civil Rights ("DHHS") notes that "[w]hile all organizations need to implement policies, procedures, and technical solutions to make it harder for hackers to gain access to their systems and data, this is

[17] https://www.ntiva.com/blog/10-cybersecurity-best-practices-for-the-healthcare-industry; Identity Theft Resource Center, 2018 End of Year Data Brach Report, https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_2018-End-of-Year-Aftermath_FINAL_V2_combinedWEB.pdf

especially important in the healthcare industry. Hackers are actively targeting healthcare organizations as they store large quantities of highly sensitive and valuable data."[18] DHHS highlights several basic cybersecurity safeguards that can be implemented to improve cyber resilience that require a relatively small financial investment, yet can have a major impact on an organization's cybersecurity posture including: (a) the proper encryption of PII AND PHI; (b) educating and training healthcare employees on how to identify social engineering attacks; (c) reviewing audit logs regularly in order to identify attempts by unauthorized individuals to gain access to PII AND PHI/PHI before they result in a data breach; and (d) correcting the configuration of software and network devices.

50. Private cyber security firms have also identified the healthcare sector as being particularly vulnerable to cyber-attacks, both because of the value of the PII and PHI they maintain and because as an industry they have been slow to adapt and respond to cybersecurity threats.[19] They too have promulgated similar best practices for bolstering cyber security and protecting against the unauthorized disclosure of PII and PHI.

51. Each of these preventative measures have long been cornerstones in industry best practices and should have been implemented before the Data Breach. These best practices were known, or should have been known by Walgreens, whose failure to heed and properly implement them directly led to the Data Breach and the unlawful exposure of PII and PHI.

I. Plaintiff and Class Members Suffered Damages

---

[18] HIPAA Journal, Cybersecurity Best Practices for Healthcare Organizations, https://www.hipaajournal.com/important-cybersecurity-best-practices-for-healthcare-organizations/

[19] See e.g., https://www.ntiva.com/blog/10-cybersecurity-best-practices-for-the-healthcare-industry; https://resources.infosecinstitute.com/category/healthcare-information-security/is-best-practices-for-healthcare/10-best-practices-for-healthcare-security/#gref

52. The ramifications of Defendant's failure to keep Patients' PII and PHI secure are long lasting and severe. Once PII and PHI is stolen, fraudulent use of that information and damage to victims may continue for years. Consumer victims of data breaches are more likely to become victims of identity fraud.[20]

53. The PII and PHI belonging to Plaintiff and Class Members is private, sensitive in nature, and was left inadequately protected by Defendant who did not obtain Plaintiff's or Class Members' consent to disclose such PII and PHI to any other person as required by applicable law and industry standards.

54. The Data Breach was a direct and proximate result of Walgreens' failure to: (a) properly safeguard and protect Plaintiff's and Class Members' PII and PHI from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and common law; (b) establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiff's and Class Members' PII and PHI; and (c) protect against reasonably foreseeable threats to the security or integrity of such information.

55. Defendant had the resources necessary to prevent the Breach, but neglected to adequately invest in data security measures, despite its obligation to protect patient data.

56. Had Defendant remedied the deficiencies in its data security systems and adopted security measures recommended by experts in the field, it would have prevented the intrusions into their systems and, ultimately, the theft of PII and PHI.

57. As a direct and proximate result of Defendant's wrongful actions and inactions, Plaintiff and Class Members have been placed at an imminent, immediate, and continuing

---

[20] 2014 LexisNexis True Cost of Fraud Study, https://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2014.pdf.

increased risk of harm from identity theft and fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and family in an effort to mitigate the actual and potential impact of the Data Breach on their lives. The U.S. Department of Justice's Bureau of Justice Statistics found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems" and that "resolving the problems caused by identity theft [could] take more than a year for some victims."[21]

58. To date, Walgreens has not offered any compensation or additional protective services to Plaintiff or Members of the Class.[22] Rather, it merely suggests that Plaintiff and Class Members change their passwords and "remain vigilant by reviewing account statements and monitoring free credit reports as a precaution."

59. This is wholly inadequate as it fails to provide any credit monitoring or fraud remediation services for victims who will face the risk of multiple years of ongoing identity theft and fraud due to the exposure. Moreover, it entirely fails to provide any compensation for the unauthorized release and disclosure of Plaintiff's and Class Members' PII and PHI.

60. As a result of the Defendant's failures to prevent the Data Breach, Plaintiff and Class Members have suffered, will suffer, or are at increased risk of suffering:

a. The compromise, publication, theft and/or unauthorized use of their PII and PHI;

b. Out-of-pocket costs associated with the prevention, detection, recovery and remediation from identity theft or fraud;

---

[21] U.S. Department of Justice, Office of Justice Programs Bureau of Justice Statistics, *Victims of Identity Theft, 2012*, December 2013 available at https://www.bjs.gov/content/pub/pdf/vit12.pdf (last visited April 19,2019).

[22] Exhibit A.

c. Lost opportunity costs and lost wages associated with efforts expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from identity theft and fraud;

d. The continued risk to their PII and PHI, which remains in the possession of Defendant and is subject to further breaches so long as Defendant fails to undertake appropriate measures to protect the PII and PHI in their possession; and

e. Current and future costs in terms of time, effort and money that will be expended to prevent, detect, contest, remediate and repair the impact of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

61. In addition to a remedy for the economic harm, Plaintiff and the Class maintain an undeniable interest in ensuring that their PII and PHI is secure, remains secure, and is not subject to further misappropriation and theft.

CLASS ACTION ALLEGATIONS

62. Plaintiff seeks relief on behalf of herself and as representatives of all others who are similarly situated. Pursuant to Fed. R. Civ. P. Rule 23(a), (b)(2), (b)(3) and (c)(4), Plaintiff seeks certification of a Nationwide class defined as follows:

> All persons whose PII and PHI was compromised as a result of the Data Breach announced by Walgreens on or about December 3, 2019 (the "Class").

63. Plaintiff also seeks certification of a Florida state-wide sub-class defined as follows:

> All persons who reside in the state of Florida whose PII and PHI was compromised as a result of the Data Breach announced by Walgreens on December 3, 2019 (the "Florida Sub-Class").

64. Excluded from the Class are Walgreens and any of its affiliates, parents or subsidiaries; all persons who make a timely election to be excluded from the Class; government entities; and the judges to whom this case is assigned, their immediate families, and court staff.

65. Plaintiff hereby reserves the right to amend or modify the class definitions with greater specificity or division after having had an opportunity to conduct discovery.

66. The proposed Class meets the criteria for certification under Rule 23(a), (b)(2), (b)(3) and (c)(4).

67. **Numerosity. Fed. R. Civ. P. 23(a)(1).** Consistent with Rule 23(a)(1), the members of the Class are so numerous and geographically dispersed that the joinder of all members is impractical. While the exact number of affected Class Members is unknown, Walgreens.com services tens of thousands of customers meeting the minimum requirements for numerosity.

68. **Commonality. Fed. R. Civ. P. 23(a)(2) and (b)(3).** Consistent with Rule 23(a)(2) and with 23(b)(3)'s predominance requirement, this action involves common questions of law and fact that predominate over any questions affecting individual Class members. The common questions include:

a. Whether Walgreens had a duty to protect patient PII and PHI;

b. Whether Walgreens knew or should have known of the susceptibility of its systems to a data breach;

c. Whether Walgreens' security measures to protect its systems were reasonable in light of best practices recommended by data security experts;

d. Whether Walgreens was negligent in failing to implement reasonable and adequate security procedures and practices;

e. Whether Walgreens' failure to implement adequate data security measures allowed the breach of its data systems to occur;

f. Whether Walgreens' conduct, including its failure to act, resulted in or was the proximate cause of the breach of its systems, resulting in the unlawful exposure of the Plaintiff's and Class Members' PII and PHI;

g. Whether Plaintiff and Class Members were injured and suffered damages or other losses because of Walgreens' failure to reasonably protect its systems and data network; and

h. Whether Plaintiff and Class members are entitled to relief.

69. **Typicality. Fed. R. Civ. P. 23(a)(3).** Consistent with Rule 23(a)(3), Plaintiff's claims are typical of those of other Class members. Plaintiff was a Walgreens customer whose PII and PHI was exposed in the Data Breach. Plaintiff's damages and injuries are akin to other Class Members, and Plaintiff seeks relief consistent with the relief sought by the Class.

70. **Adequacy. Fed. R. Civ. P. 23(a)(4).** Consistent with Rule 23(a)(4), Plaintiff is an adequate representative of the Class because Plaintiff: (1) is a member of the Class she seeks to represent; (2) is committed to pursuing this matter against Walgreens to obtain relief for the Class; and (3) has no conflicts of interest with the Class. Moreover, Plaintiff's Counsel are competent and experienced in litigating class actions, including privacy litigation of this kind.

Plaintiff intends to vigorously prosecute this case and will fairly and adequately protect the Class' interests.

71. **Superiority. Fed. R. Civ. P. 23(b)(3).** Consistent with Rule 23(b)(3), a class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The quintessential purpose of the class action mechanism is to permit litigation against wrongdoers even when damages to an individual plaintiff may not be sufficient to justify individual litigation. Here, the damages suffered by Plaintiff and the Class are relatively small compared to the burden and expense required to individually litigate their claims against Walgreens, and thus, individual litigation to redress Walgreens' wrongful conduct would be impracticable. Individual litigation by each Class member would also strain the court system. Individual litigation creates the potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court.

72. **Injunctive and Declaratory Relief.** Class certification is also appropriate under Rule 23(b)(2). Defendant, through its uniform conduct, acted or 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.

73. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Walgreens failed to timely notify the public of the Data Breach;

b. Whether Walgreens owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their PII and PHI;

c. Whether Walgreens' security measures to protect its data systems were reasonable in light of best practices recommended by data security experts;

d. Whether Defendant's failure to institute adequate protective security measures amounted to negligence;

e. Whether Defendant failed to take commercially reasonable steps to safeguard patient PII and PHI;

f. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the data breach; and

g. Whether Walgreens filed to comply with its obligations under HIPAA.

74. Finally, all members of the proposed Classes are readily ascertainable. Walgreens has access to patient names and addresses affected by the Data Breach. Using this information, Class members can be identified and ascertained for the purpose of providing notice.

FIRST CAUSE OF ACTION
NEGLIGENCE
(On Behalf of Plaintiff and the Nationwide Class)

75. Plaintiff restates and realleges paragraphs 1 through 74 above as if fully set forth herein.

76. As a condition of receiving services, Plaintiff and Class Members were obligated to provide Walgreens with their PII and PHI.

77. Plaintiff and the Class Members entrusted their PII and PHI to Walgreens with the understanding that Walgreens would safeguard their information.

78. Defendant had full knowledge of the sensitivity of the PII and PHI and the types of harm that Plaintiff and Class Members could and would suffer if the PII and PHI were wrongfully disclosed.

79. Defendant had a duty to exercise reasonable care in safeguarding, securing and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining and testing the Defendant's security protocols to ensure that PII and PHI in its possession was adequately secured and protected and that employees tasked with maintaining such information were adequately training on cyber security measures regarding the security of such information.

80. Plaintiff and the Class Members were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew of or should have known of the inherent risks in collecting and storing the PII and PHI of Plaintiff and the Class, the critical importance of providing adequate security of that PII and PHI, the current cyber scams being perpetrated and that it had inadequate employee training and education and IT security protocols in place to secure the PII and PHI of Plaintiff and the Class.

81. Defendant's own conduct created a foreseeable risk of harm to Plaintiff and Class Members. Defendant's misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included its decision not to comply with HIPAA and industry standards for the safekeeping and encrypted authorized disclosure of the PII and PHI of Plaintiff and Class Members.

82. Plaintiff and the Class Members had no ability to protect their PII and PHI that was in Walgreens' possession.

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

84. Defendant had a duty to put proper procedures in place in order to prevent the unauthorized dissemination of Plaintiff and Class Members' PII and PHI.

85. Defendant has admitted that Plaintiff's and Class Members' PII and PHI was wrongfully disclosed to unauthorized third persons as a result of the Data Breach.

86. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class Members by failing to exercise reasonable care in protecting and safeguarding the Plaintiff's and Class Members' PII and PHI while it was within the Walgreens' possession or control.

87. Defendant improperly and inadequately safeguarded Plaintiff's and Class Members' PII and PHI in deviation of standard industry rules, regulations and practices at the time of the Data Breach.

88. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class Members by failing to have appropriate procedures in place to detect and prevent dissemination of its patients' PII and PHI.

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

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

91. There is a temporal and close causal connection between Defendant's failure to implement security measures to protect the PII and PHI and the harm suffered, or risk of imminent harm suffered by Plaintiff and the Class.

92. As a result of Defendant's negligence, Plaintiff and the Class Members have suffered and will continue to suffer damages and injury including, but not limited to: out-of-pocket expenses associated with procuring robust identity protection and restoration services; increased risk of future identity theft and fraud, the costs associated therewith; time spent monitoring, addressing and correcting the current and future consequences of the Data Breach; and the necessity to engage legal counsel and incur attorneys' fees, costs and expenses.

SECOND CAUSE OF ACTION
NEGLIGENCE *PER SE*
(On Behalf of Plaintiff and the Nationwide Class)

93. Plaintiff restates and realleges Paragraphs 1 through 74 as if fully set forth herein.

94. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Walgreens, of failing to use reasonable measures to protect PII and PHI. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

95. Walgreens violated Section 5 of the FTC Act by failing to use reasonable measures to protect patient PII and PHI and not complying with applicable industry standards, as described in detail herein. Walgreens' conduct was particularly unreasonable given the nature and amount of PII and PHI it obtained and stored, and the foreseeable consequences of a data breach including, specifically, the damages that would result to Plaintiff and Class Members.

96. Walgreens' violation of Section 5 of the FTC Act constitutes negligence *per se*.

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

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

99. As a direct and proximate result of Walgreens' negligence *per se*, Plaintiff and the Class have suffered, and continue to suffer, injuries and damages arising from the Data Breach including, but not limited to: damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives, including, *inter alia*, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial and medical accounts, closely reviewing and monitoring their credit reports and various accounts for unauthorized activity, and filing police reports, and damages from identity theft, which may take months if not years to discover and detect.

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

THIRD CAUSE OF ACTION
INVASION OF PRIVACY
(On Behalf of Plaintiff and the Nationwide Class)

101. Plaintiff restates and realleges paragraphs 1 through 74 above as if fully set forth herein.

102. Plaintiff and Class Members had a legitimate expectation of privacy with respect to their PII and PHI and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

103. Defendant owed a duty to patients in its network, including Plaintiff and Class Members, to keep their PII and PHI confidential.

104. The unauthorized release of PII and PHI, especially the type related to personal health information, is highly offensive to a reasonable person.

105. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiff and Class Members disclosed their PII and PHI to Defendant as part of their use of Walgreens' services, but privately, with the intention that the PII and PHI would be kept confidential and protected from unauthorized disclosure. Plaintiff and Class Members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

106. The Data Breach constitutes an intentional interference with Plaintiff and Class Members' interest in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

107. Defendant acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

108. Acting with knowledge, Walgreens had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiff and Class Members.

109. As a proximate result of Defendant's acts and omissions, Plaintiff's and Class Members' PII and PHI was disclosed to and used by third parties without authorization, causing Plaintiff and Class Members to suffer damages.

110. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and Class Members in that the PII and PHI maintained by Defendant can be viewed, distributed, and used by unauthorized persons.

111. Plaintiff and Class Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiff and the Class.

FOURTH CAUSE OF ACTION
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Nationwide Class)

112. Plaintiff restates and realleges paragraphs 1 through 74 above as if fully set forth herein.

113. Plaintiff and Class Members were required to provide their PII and PHI to Defendant as a condition of their use of Defendant's services.

114. Plaintiff and Class Members paid money, or money was paid on their behalf, to Defendant in exchange for services, along with Defendant's promise to protect their health information and other PII and PHI from unauthorized disclosure.

115. In its written privacy policies, Walgreens expressly promised Plaintiff and Class Members that it would only disclose protected health information and other PII and PHI under certain circumstances, none of which relate to the Data Breach.

116. Walgreens promised to comply with HIPAA standards and to make sure that Plaintiff's and Class Members' health information and other PII and PHI would remain protected.

117. Implicit in the agreement between Plaintiff and Class Members and the Defendant to provide protected health information and other PII and PHI, was the latter's obligation to: (a) use such PII and PHI for business purposes only; (b) take reasonable steps to safeguard that PII and PHI; (c) prevent unauthorized disclosures of the PII and PHI; (d) provide Plaintiff and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their PII and PHI; (e) reasonably safeguard and protect the PII and PHI of Plaintiff and Class Members from unauthorized disclosure or uses; (f) retain the PII and PHI only under conditions that kept such information secure and confidential.

118. Without such implied contracts, Plaintiff and Class Members would not have provided their PII and PHI to Defendant.

119. Plaintiff and Class Members fully performed their obligations under the implied contract with Defendant, however, Defendant did not.

120. Defendant breached the implied contracts with Plaintiff and Class Members by failing to:

a. reasonably safeguard and protect Plaintiff and Class Members' PII and PHI, which was compromised as a result of the Data Breach;

b. comply with their promise to abide by HIPAA;

c. ensure the confidentiality and integrity of electronic protected health information Defendant created, received, maintained, and transmitted in violation of 45 C.F.R. § 164.306(a)(1);

d. implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

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

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

g. to protect against any reasonably anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45 C.F.R. § 164.306(a)(2).

FIFTH CAUSE OF ACTION
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Nationwide Class)

121. Plaintiff restates and realleges paragraphs 1 through 74 above as if fully set forth herein.

122. Plaintiff and Class Members conferred a monetary benefit on Defendant. Specifically, they purchased goods and services from Defendant and in so doing provided Defendant with their PII and PHI. In exchange, Plaintiff and Class Members should have

received from Defendant the goods and services that were the subject of the transaction and have their PII and PHI protected with adequate data security.

123. Defendant knew that Plaintiff and Class Members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the PII and PHI of Plaintiff and Class Members for business purposes.

124. The amounts Plaintiff and Class Members paid for goods and services were used, in part, to pay for use of Defendant's network and the administrative costs of data management and security.

125. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

126. Defendant failed to secure Plaintiff's and Class Members' PII and PHI and, therefore, did not provide full compensation for the benefit Plaintiff and Class Members provided.

127. Defendant acquired the PII and PHI through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

128. If Plaintiff and Class Members knew that Defendant had not secured their PII and PHI, they would not have agreed to Defendant's services.

129. Plaintiff and Class Members have no adequate remedy at law.

130. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII and PHI is used; (iii) the compromise,

publication, and/or theft of their PII and PHI; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII and PHI; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their PII and PHI, 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 PII and PHI in their continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII and PHI compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

131. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

132. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiff and Class Members overpaid for Defendant's services.

SIXTH CAUSE OF ACTION
BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiff and the Nationwide Class)

133. Plaintiff restates and realleges paragraphs 1 through 74 above as if fully set forth herein.

134. In light of their special relationship, Defendant has become the guardian of Plaintiff and Class Member's PII and PHI. Defendant has become a fiduciary, created by its undertaking and guardianship of patient PII and PHI, to act primarily for the benefit of its

patients, including Plaintiff and Class Members. This duty included the obligation to safeguard Plaintiff and Class Member PII and PHI and to timely notify them in the event of a data breach.

135. Defendant has a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of its relationship. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to:

a. properly encrypt and otherwise protect the integrity of the system containing Plaintiff's and Class Members' protected health information and other PII and PHI;

b. timely notify and/or warn Plaintiff and Class Members of the Data Breach.

c. ensure the confidentiality and integrity of electronic protected health information Defendant created, received, maintained, and transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

d. implement technical policies and procedures to limit access to only those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

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

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

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

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

i. ensure compliance with the HIPAA security standard rules by their workforce in violation of 45 C.F.R. § 164.306(a)(94).

j. prevent the use and disclosure of protected health information that is and remains accessible to unauthorized persons in violation of 45 C.F.R. § 164.502, et seq.;

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

l. design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard protected health information, in compliance with 45 C.F.R. § 164.530(c).

m. otherwise failing to safeguard Plaintiff's and Class Members' PII AND PHI.

136. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII and PHI is used; (iii) the

compromise, publication, and/or theft of their PII and PHI; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their PII and PHI; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their PII and PHI, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Patient PII and PHI in its continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII and PHI compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

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

SEVENTH CAUSE OF ACTION
VIOLATION OF THE FLORIDA UNFAIR AND DECEPTIVE TRADE PRACTICES ACT, Fla. Stat. §§ 501.201, *et seq.*
(On Behalf of Plaintiff and the Florida Subclass)

138. Plaintiff restates and realleges paragraphs 1 through 74 above as if fully set forth herein.

139. Walgreens operating in Florida engaged in unconscionable, unfair, and deceptive acts and practices in the conduct of trade and commerce, in violation of Fla. Stat. § 501.204(1). This includes but is not limited to the following:

a. Failing to enact adequate privacy and security measures to protect Florida Subclass Members' PII and PHI from unauthorized disclosure, release,

data breaches, and theft, which was a direct and proximate cause of the Walgreens Data Breach;

b. Failing to take proper action following known security risks and prior cybersecurity incidents, which was a direct and proximate cause of the Walgreens Data Breach;

c. Knowingly and fraudulently misrepresenting that it would maintain adequate data privacy and security practices and procedures to safeguard Florida Subclass Members' PII and PHI from unauthorized disclosure, release, data breaches, and theft;

d. Knowingly omitting, suppressing, and concealing the inadequacy of its privacy and security protections for Florida Subclass Members' PII and PHI;

e. Knowingly and fraudulently misrepresenting that it would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Florida Subclass Members' PII and PHI;

f. Failing to maintain the privacy and security of Florida Subclass Members' PII and PHI, in violation of duties imposed by applicable federal and state laws, including but not limited to those mentioned in the foregoing paragraph, which was a direct and proximate cause of the Walgreens Data Breach; and

g. Failing to disclose the Walgreens Data Breach to Florida Subclass Members in a timely and accurate manner, in violation of Fla. Stat. § 501.171(4).

140. As a direct and proximate result of Walgreens' practices, Florida Subclass Members suffered the injury and/or damages described herein, including but not limited to time and expenses related to monitoring their financial accounts for fraudulent activity, an increased, imminent risk of fraud and identity theft, and loss of value of their Personal Information.

141. The above unfair and deceptive practices and acts by Walgreens were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to the Florida Subclass Members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

142. Walgreens knew or should have known that its computer systems and data security practices were inadequate to safeguard Florida Subclass Members' PII and PHI and that the risk of a data breach or theft was high. Walgreens' actions were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of Florida Subclass Members.

143. Plaintiff and Florida Subclass Members seek actual damages under Fla. Stat. § 501.211(2), and attorneys' fees under Fla. Stat. § 501.2105(1), to be proven at trial.

144. Plaintiff and Florida Subclass Members also seek an order enjoining Walgreens' unfair, unlawful, and/or deceptive practices, declaratory relief, and any other just and proper relief available under the Florida Deceptive and Unfair Trade Practices Act, Fla. Stat. §§ 501.201, *et seq*

WHEREFORE, Plaintiff, on behalf of herself and all others similarly situated, respectfully requests the following relief:

a. An Order certifying this case as a class action;

b. An Order appointing Plaintiff as the class representative;

c. An Order appointing undersigned counsel as class counsel;

d. A mandatory injunction directing the Defendant to hereinafter adequately safeguard the PII and PHI of the Class by implementing improved security procedures and measures;

e. An award of damages;

f. An award of costs and expenses;

g. An award of attorneys' fees; and

h. Such other and further relief as this court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff demands a jury trial as to all issues triable by a jury.

Dated: April 20, 2020

Respectfully submitted,

by: */s/ Carl V. Malmstrom*

Carl V. Malmstrom
WOLF HALDENSTEIN ADLER FREEMAN & HERZ LLC
111 W. Jackson Street, Suite 1700
Chicago, IL 60604
Tel: (312) 391-5059
Fax: (212) 545-4653
malmstrom@whafh.com

Local Counsel for Plaintiff

Jean Martin
Ryan McGee
MORGAN & MORGAN COMPLEX LITIGATION GROUP
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
Telephone: (813) 223-5505
Facsimile: (813) 223-5402
jeanmartin@forthepeople.com
rmcgee@forthepeople.com

Attorneys for Plaintiff and the Putative Class

whafhch55986

ClassAction.org