IN THE UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF KENTUCKY
SOUTHERN DIVISION
LONDON DOCKET

CARLA SMITH, individually, and on behalf of all others similarly situated, Plaintiff, v. BHG XXXIV, LLC and BHG HOLDINGS, LLC, d/b/a BEHAVIORAL HEALTH GROUP, Defendants.	CLASS ACTION JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiff Carla Smith ("Plaintiff"), individually, and on behalf of all others similarly situated (collectively, "Class members"), by and through her attorneys, brings this Class Action Complaint against Defendants BHG XXXIV, LLC and BHG Holdings, LLC, d/b/a Behavioral Health Group (together, "BHG") and complains and alleges upon personal knowledge as to herself and information and belief as to all other matters.

INTRODUCTION

1. Plaintiff brings this class action against BHG for its failure to secure and safeguard her and approximately 197,507 other individuals' personally identifying information ("PII") and personal health information ("PHI"), including name, Social Security number, driver's license or state identification number, financial account information, payment card information, passport, biometrics, health insurance information, and medical information.

2. BHG is a company that provides rehabilitation and other services to persons dealing with opioid addiction and their families. BHG XXXIV, LLC is a subsidiary of BHG Holdings,

LLC. BHG XXXIV, LLC's principal office is located in Corbin, Kentucky. BHG Holdings, LLC has its principal place of business in Dallas, Texas.

3. On or about December 5, 2021, unauthorized individuals gained access to BHG's network systems and accessed and acquired files from the system that contained the PII/PHI of Plaintiff and Class members (the "Data Breach").

4. BHG owed a duty to Plaintiff and Class members to implement and maintain reasonable and adequate security measures to secure, protect, and safeguard their PII/PHI against unauthorized access and disclosure. BHG breached that duty by, among other things, failing to implement and maintain reasonable security procedures and practices to protect its patients', former patients', employees', and former employees' PII/PHI from unauthorized access and disclosure.

5. As a result of BHG's inadequate security and breach of its duties and obligations, the Data Breach occurred, and Plaintiff's and Class members' PII/PHI was accessed and disclosed. This action seeks to remedy these failings and their consequences. Plaintiff brings this action on behalf of herself and all persons whose PII/PHI was exposed as a result of the Data Breach, which BHG says it learned of on or about December 5, 2021, and first publicly acknowledged on or about July 27, 2022, over seven months after the breach was allegedly discovered.

6. Plaintiff, on behalf of herself and all other Class members, asserts claims for negligence, negligence per se, breach of fiduciary duty, breach of express contract, breach of implied contract, and unjust enrichment, and seeks declaratory relief, injunctive relief, monetary damages, statutory damages, punitive damages, equitable relief, and all other relief authorized by law.

PARTIES

7. Plaintiff Carla Smith is a Kentucky resident. She was formerly employed by BHG and worked at BHG's Corbin, Kentucky location. She received a letter from BHG dated July 27, 2022, notifying her that files and folders containing her PII/PHI were removed from BHG's network in the Data Breach. Plaintiff Smith would not have sought employment from or provided her PII/PHI to BHG had she known that her information would not be adequately safeguarded by BHG.

8. Defendant BHG XXXIV, LLC is a limited liability company formed in Kentucky. BHG XXXIV, LLC's principal place of business is the Corbin Treatment Center, which is located at 785 Cumberland Gap Parkway, Suite 3, Corbin, KY 40701. BHG XXXIV, LLC may be served through its registered agent: CT Corporation System, 306 W. Main Street, Suite 512, Frankfort, Kentucky 40601.

9. Defendant BHG Holdings, LLC is a limited liability company formed in Texas. BHG Holdings, LLC's principal place of business is 5001 Spring Valley Road, Suite 600E, Dallas, Texas 75244. BHG Holdings, LLC may be served through its registered agent: Rajinder Singh, 3023 E Hwy 80, Odessa, Texas 79761.

JURISDICTION AND VENUE

10. The Court has subject matter jurisdiction over Plaintiff's claims under 28 U.S.C. § 1332(d)(2), because (a) there are 100 or more Class members, (b) at least one Class member is a citizen of a state that is diverse from the citizenship of all of Defendant's members, and (c) the matter in controversy exceeds $5,000,000, exclusive of interest and costs.

11. This Court has personal jurisdiction over BHG XXXIV, LLC because BHG XXXIV, LLC has its principal place of business in Kentucky.

12. This Court has personal jurisdiction over BHG Holdings, LLC because BHG Holdings, LLC does business in this state and the causes of action arose as a result of BHG Holdings, LLC's business in the state.

13. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(2) because BHG XXXIV, LLC's principal place of business is in Corbin, Kentucky, BHG Holdings, LLC does business in this District through its subsidiary, BHG XXXIV, LLC, and a significant amount of the events leading to Plaintiff's causes of action occurred in this District.

FACTUAL ALLEGATIONS

Overview of BHG

14. BHG provides services to persons dealing with drug addiction. In some instances, BHG administers or prescribes medication to its patients and provides psychological therapy services.[1]

15. In the regular course of its business, BHG collects and maintains the PII/PHI of its patients and its employees.

16. BHG provides its patients with its Notice of Privacy Practices. The Notice of Privacy Practices states, "BHG is committed to fully complying with HIPAA and with the protection of your health information."[2] The notice goes on to state, "We are required by law to maintain the privacy of your health information and provide you notice of our legal duties and privacy practices with respect to your health information. We will abide by the terms of this Notice." *Id*.

---

[1] *Patients and Families*, BEHAVIORAL HEALTH GROUP, https://www.bhgrecovery.com/patients-and-families (last accessed Sep. 2, 2022).
[2] *BHG Notice of Privacy Practices*, BEHAVIORAL HEALTH GROUP, https://f.hubspotusercontent10.net/hubfs/7851312/NOTICE-OF-PRIVACY-PRACTICES.pdf (last accessed Sep. 2, 2022).

17. Plaintiff and Class members are, or were, patients or employees of BHG and entrusted BHG with their PII/PHI.

The Data Breach

18. On or about December 5, 2021, an unauthorized individual, or unauthorized individuals, gained access to BHG's network systems and accessed and acquired certain files on BHG's computer systems.

19. BHG did not begin to notify government agencies or the public about the data breach until over seven months after that, on or about July 27, 2022. The notice that BHG posted to its website states that the information that the cybercriminal had access to includes the following PII/PHI: "full name, Social Security number, driver's license or state identification number, financial account information, payment card information, passport, biometrics, health insurance information and/or medical information including medical diagnosis and treatment, medication information, dates of service, and/or medical record number."[3]

20. The information involved in the Data Breach is especially sensitive because of the nature of BHG's business, which is providing rehabilitation services to persons dealing with substance abuse.

21. BHG's notice states that its investigation into the Data Breach revealed on June 22, 2022, that files and folders containing PII/PHI related to Plaintiff and Class members "may have been accessed or acquired."[4] Despite this, BHG still waited an additional month to tell its patients, former patients, employees, and former employees that the breach occurred.

---

[3] *BHG Holdings, LLC dba Behavioral Health Group Provides Notice of Data Security Incident*, BEHAVIORAL HEALTH GROUP, https://www.bhgrecovery.com/bhg-hipaa-substitute-notice (last accessed Sep. 2, 2022).
[4] *Id*.

BHG Knew that Criminals Target PII/PHI

22. At all relevant times, BHG knew, or should have known, that the PII/PHI that it collected was a target for malicious actors. Despite such knowledge, BHG failed to implement and maintain reasonable and appropriate data privacy and security measures to protect Plaintiff's and Class members' PII/PHI from cyber-attacks that BHG should have anticipated and guarded against.

23. It is well known amongst companies that store sensitive personally identifying information that sensitive information—such as the Social Security numbers ("SSNs") and medical information stolen in the Data Breach—is valuable and frequently targeted by criminals. In a recent article, *Business Insider* noted that "[d]ata breaches are on the rise for all kinds of businesses, including retailers . . . . Many of them were caused by flaws in . . . systems either online or in stores."[5]

24. Cyber criminals seek out PHI at a greater rate than other sources of personal information. In a 2022 report, the healthcare compliance company Protenus found that there were 905 medical data breaches in 2021 with over 50 million patient records exposed.[6] This is an increase from the 758 medical data breaches which exposed approximately 40 million records that Protenus compiled in 2020.[7]

[5] Dennis Green, Mary Hanbury & Aine Cain, *If you bought anything from these 19 companies recently, your data may have been stolen*, BUSINESS INSIDER (Nov. 19, 2019, 8:05 A.M.), https://www.businessinsider.com/data-breaches-retailers-consumer-companies-2019-1.
[6] PROTENUS, *2022 Breach Barometer*, PROTENUS.COM, https://www.protenus.com/breach-barometer-report (last accessed Sep. 2, 2022).
[7] *Id*.

25. PII/PHI is a valuable property right.[8] The value of PII/PHI as a commodity is measurable.[9] "Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory frameworks."[10] American companies are estimated to have spent over $19 billion on acquiring personal data of consumers in 2018.[11] It is so valuable to identity thieves that once PII/PHI has been disclosed, criminals often trade it on the "cyber black-market," or the "dark web," for many years.

26. As a result of their real and significant value, identity thieves and other cyber criminals have openly posted credit card numbers, SSNs, PII/PHI, and other sensitive information directly on various Internet websites making the information publicly available. This information from various breaches, including the information exposed in the Data Breach, can be readily aggregated and become more valuable to thieves and more damaging to victims.

---

[8] *See* Marc van Lieshout, *The Value of Personal Data*, 457 International Federation for Information Processing 26 (May 2015) ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible…"), https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data.

[9] *See* Robert Lowes, *Stolen EHR [Electronic Health Record] Charts Sell for $50 Each on Black Market*, MEDSCAPE.COM (April 28, 2014), http://www.medscape.com/viewarticle/824192.

[10] OECD, *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD ILIBRARY (April 2, 2013), https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en.

[11] IAB Data Center of Excellence, *U.S. Firms to Spend Nearly $19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017*, IAB.COM (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/.

27. PHI is particularly valuable and has been referred to as a "treasure trove for criminals."[12] A cybercriminal who steals a person's PHI can end up with as many as "seven to ten personal identifying characteristics of an individual."[13]

28. All-inclusive health insurance dossiers containing sensitive health insurance information, names, addresses, telephone numbers, email addresses, SSNs, and bank account information, complete with account and routing numbers, can fetch up to $1,200 to $1,300 each on the black market.[14] According to a report released by the Federal Bureau of Investigation's ("FBI") Cyber Division, criminals can sell healthcare records for 50 times the price of a stolen Social Security or credit card number.[15]

29. Criminals can use stolen PII/PHI to extort a financial payment by "leveraging details specific to a disease or terminal illness."[16] Quoting Carbon Black's Chief Cybersecurity Officer, one recent article explained: "Traditional criminals understand the power of coercion and extortion . . . By having healthcare information—specifically, regarding a sexually transmitted disease or terminal illness—that information can be used to extort or coerce someone to do what you want them to do."[17]

---

[12] *See* Andrew Steager, *What Happens to Stolen Healthcare Data*, HEALTHTECH MAGAZINE (Oct. 20, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon ("*What Happens to Stolen Healthcare Data*") (quoting Tom Kellermann, Chief Cybersecurity Officer, Carbon Black, stating "Health information is a treasure trove for criminals.").

[13] *Id.*

[14] SC Staff, *Health Insurance Credentials Fetch High Prices in the Online Black Market*, SC MAGAZINE (July 16, 2013), https://www.scmagazine.com/news/breach/health-insurance-credentials-fetch-high-prices-in-the-online-black-market.

[15] Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain* (April 8, 2014), https://www.illuminweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systems-cyber-intrusions.pdf (last accessed Sep. 2, 2022).

[16] *What Happens to Stolen Healthcare Data*, *supra* at n.12.

[17] *Id.*

30. Consumers place a high value on the privacy of that data, as they should. Researchers shed light on how much consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[18]

31. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' PII/PHI has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

Theft of PII/PHI Has Grave and Lasting Consequences for Victims

32. Theft of PII/PHI is serious. The FTC warns consumers that identity thieves use PII/PHI to exhaust financial accounts, receive medical treatment, start new utility accounts, and incur charges and credit in a person's name.[19]

33. Identity thieves use personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[20] According to Experian, one of the largest credit reporting companies in the world, "[t]he research shows that personal information is

[18] Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior*, *An Experimental Study*, 22(2) INFORMATION SYSTEMS RESEARCH 254 (June 2011) https://www.jstor.org/stable/23015560?seq=1.

[19] *See* Federal Trade Commission, *What to Know About Identity Theft*, FEDERAL TRADE COMMISSION CONSUMER INFORMATION, https://www.consumer.ftc.gov/articles/what-know-about-identity-theft (last accessed Sep. 2, 2022).

[20] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 C.F.R. § 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*.

valuable to identity thieves, and if they can get access to it, they will use it" to among other things: open a new credit card or loan; change a billing address so the victim no longer receives bills; open new utilities; obtain a mobile phone; open a bank account and write bad checks; use a debit card number to withdraw funds; obtain a new driver's license or ID; use the victim's information in the event of arrest or court action.[21]

34. With access to an individual's PII/PHI, criminals can do more than just empty a victim's bank account—they can also commit all manner of fraud, including: obtaining a driver's license or official identification card in the victim's name but with the thief's picture; using the victim's name and SSN to obtain government benefits; or, filing a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's SSN, rent a house, or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest, resulting in an arrest warrant being issued in the victim's name.[22]

35. Identity theft is not an easy problem to solve. In a survey, the Identity Theft Resource Center found that most victims of identity crimes need more than a month to resolve issues stemming from identity theft and some need over a year.[23]

36. Theft of SSNs also creates a particularly alarming situation for victims because those numbers cannot easily be replaced. In order to obtain a new number, a breach victim has to

---

[21] *See* Susan Henson, *What Can Identity Thieves Do with Your Personal Information and How Can You Protect Yourself*, EXPERIAN, https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/ (last accessed Sep. 2, 2022).

[22] *See* Federal Trade Commission, *Warning Signs of Identity Theft*, IDENTITYTHEFT.GOV https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft (last accessed Sep. 2, 2022).

[23] Identity Theft Resource Center, *2021 Consumer Aftermath Report*, IDENTITY THEFT RESOURCE CENTER (2021), https://www.idtheftcenter.org/identity-theft-aftermath-study/ (last accessed Sep. 2, 2022).

demonstrate ongoing harm from misuse of her SSN, and a new SSN will not be provided until after the harm has already been suffered by the victim.

37. Due to the highly sensitive nature of SSNs, theft of SSNs in combination with other PII (e.g., name, address, date of birth) is akin to having a master key to the gates of fraudulent activity. TIME quotes data security researcher Tom Stickley, who is employed by companies to find flaws in their computer systems, as stating, "If I have your name and your Social Security number and you don't have a credit freeze yet, you're easy pickings."[24]

38. Theft of PII is even more serious when it includes theft of PHI. Data breaches involving medical information "typically leave[] a trail of falsified information in medical records that can plague victims' medical and financial lives for years."[25] It "is also more difficult to detect, taking almost twice as long as normal identity theft."[26] In warning consumers on the dangers of medical identity theft, the FTC states that an identity thief may use PII/PHI "to see a doctor, get prescription drugs, buy medical devices, submit claims with your insurance provider, or get other medical care." [27] The FTC also warns, "If the thief's health information is mixed with yours it could affect the medical care you're able to get or the health insurance benefits you're able to

[24] Patrick Lucas Austin, *'It Is Absurd.' Data Breaches Show it's Time to Rethink How We Use Social Security Numbers, Experts Say*, TIME (August 5, 2019), https://time.com/5643643/capital-one-equifax-data-breach-social-security/.
[25] Pam Dixon and John Emerson, *The Geography of Medical Identity Theft*, FTC.GOV (Dec. 12, 2017), http://www.worldprivacyforum.org/wp-content/uploads/2017/12/WPF_Geography_of_Medical_Identity_Theft_fs.pdf.
[26] *See* Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk…*, *supra* at n.15.
[27] *See* Federal Trade Commission, *What to Know About Medical Identity Theft*, Federal Trade Commission Consumer Information, https://www.consumer.ftc.gov/articles/what-know-about-medical-identity-theft (last accessed Sep. 2, 2022).

use."[28]

39. A report published by the World Privacy Forum and presented at the US FTC Workshop on Informational Injury describes what medical identity theft victims may experience:

- Changes to their health care records, most often the addition of falsified information, through improper billing activity or activity by imposters. These changes can affect the healthcare a person receives if the errors are not caught and corrected.
- Significant bills for medical goods and services not sought nor received.
- Issues with insurance, co-pays, and insurance caps.
- Long-term credit problems based on problems with debt collectors reporting debt due to identity theft.
- Serious life consequences resulting from the crime; for example, victims have been falsely accused of being drug users based on falsified entries to their medical files; victims have had their children removed from them due to medical activities of the imposter; victims have been denied jobs due to incorrect information placed in their health files due to the crime.
- As a result of improper and/or fraudulent medical debt reporting, victims may not qualify for mortgage or other loans and may experience other financial impacts.
- Phantom medical debt collection based on medical billing or other identity information.
- Sales of medical debt arising from identity theft can perpetuate a victim's debt collection and credit problems, through no fault of their own.[29]

40. There may also be a time lag between when sensitive personal information is stolen, when it is used, and when a person discovers it has been used. For example, on average it takes approximately three months for consumers to discover their identity has been stolen and used, but it takes some individuals up to three years to learn that information.[30]

---

[28] *Id*.
[29] *See* Pam Dixon and John Emerson, *The Geography of Medical Identity Theft*, *supra* at n.25.
[30] John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 Journal of Systemics, Cybernetics and Informatics 9 (2019), http://www.iiisci.org/journal/pdv/sci/pdfs/IP069LL19.pdf.

41. It is within this context that Plaintiff and Class members must now live with the knowledge that their PII/PHI is forever in cyberspace and was taken by and in the possession of people willing to use the information for any number of improper purposes and scams, including making the information available for sale on the black-market.

Damages Sustained by Plaintiff and the Other Class Members

42. Plaintiff and Class members have suffered and will suffer injury, including, but not limited to: (i) a substantial increase in the likelihood of identity theft; (ii) the compromise, publication, and theft of their PII/PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with effort attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI which remains in BHG's possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII/PHI compromised as a result of the Data Breach; and (vii) overpayment for the services that were received without adequate data security.

CLASS ALLEGATIONS

43. This action is brought and may be properly maintained as a class action pursuant to Rule 23 of the Federal Rules of Civil Procedure.

44. Plaintiff brings this action on behalf of herself and all members of the following Nationwide Class of similarly situated persons:

> All persons whose PHI/PII was disclosed to unauthorized persons in the Data Breach, including all persons who were sent a notice of the Data Breach (the "Nationwide Class").

45. Plaintiff alternatively brings this action on behalf of herself and all members of the following subclass of similarly situated persons:

> All persons who have received services from or have been employed by BHG XXXIV, LLC and whose PII/PHI was disclosed to unauthorized persons in the Data Breach, including all persons who received services from or were employed by BHG XXXIV, LLC and were sent a notice of the Data Breach (the "XXXIV Subclass").[31]

46. Excluded from the Class is BHG XXXIV, LLC and BHG Holdings, LLC and their affiliates, parents, subsidiaries, officers, agents, and directors, as well as the judge(s) presiding over this matter and the clerks of said judge(s).

47. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of her 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.

48. The members in the Class are so numerous that joinder of each of the Class members in a single proceeding would be impracticable. BHG reported to the United States Department of Health and Human Services Office of Civil Rights that approximately 197,507 persons' information was exposed in the Data Breach.

49. Common questions of law and fact exist as to all Class members and predominate over any potential questions affecting only individual Class members. Such common questions of law or fact include, *inter alia*:

a. Whether BHG had a duty to implement and maintain reasonable security procedures and practices to protect and secure Plaintiff's and Class Members' PII/PHI from unauthorized access and disclosure;

b. Whether BHG failed to exercise reasonable care to secure and safeguard Plaintiff's and Class Members' PII/PHI;

[31] The Nationwide Class and the XXXIV Subclass are collectively referred to as the "Class."

c. Whether an implied contract existed between Class members and BHG, providing that BHG would implement and maintain reasonable security measures to protect and secure Class Members' PII/PHI from unauthorized access and disclosure;

d. Whether BHG breached its duties to protect Plaintiff's and Class members' PII/PHI; and

e. Whether Plaintiff and Class members are entitled to damages and the measure of such damages and relief.

50. BHG engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff, on behalf of herself and all other Class members. Individual questions, if any, pale in comparison, in both quantity and quality, to the numerous common questions that dominate this action.

51. Plaintiff's claims are typical of the claims of the Class. Plaintiff, like all proposed members of the Class, had her PII/PHI compromised in the Data Breach. Plaintiff and Class members were injured by the same wrongful acts, practices, and omissions committed by BHG, as described herein. Plaintiff's claims therefore arise from the same practices or course of conduct that give rise to the claims of all Class members.

52. Plaintiff will fairly and adequately protect the interests of the Class members. Plaintiff is an adequate representative of the Class in that she has no interests adverse to, or that conflict with, the Class she seeks to represent. Plaintiff has retained counsel with substantial experience and success in the prosecution of complex consumer protection class actions of this nature.

53. 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 damages and other financial detriment suffered by Plaintiff and Class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against BHG, so it would be impracticable for Class members to individually seek redress from BHG's wrongful conduct. Even if Class members could afford individual litigation, the court system could not. Individualized litigation creates a 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 single adjudication, economy of scale, and comprehensive supervision by a single court.

CAUSES OF ACTION

COUNT I
NEGLIGENCE

54. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

55. Plaintiff brings this claim against BHG Holdings, LLC on behalf of both the Nationwide Class and the XXXIV Subclass and brings this claim against BHG XXXIV, LLC on behalf of the XXXIV Subclass.

56. BHG owed a duty to Plaintiff and Class members to exercise reasonable care in safeguarding and protecting their PII/PHI in its possession, custody, or control.

57. BHG knew the risks of collecting and storing Plaintiff's and all other Class members' PII/PHI and the importance of maintaining secure systems. BHG knew of the many data breaches that targeted companies that stored PII/PHI in recent years.

58. Given the nature of BHG's business, the sensitivity and value of the PII/PHI it maintains, and the resources at its disposal, BHG should have identified the vulnerabilities to their systems and prevented the Data Breach from occurring.

59. BHG breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII/PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect PII/PHI entrusted to it—including Plaintiff's and Class members' PII/PHI.

60. It was reasonably foreseeable to BHG that its failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII/PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems would result in the unauthorized release, disclosure, and dissemination of Plaintiff's and Class members' PII/PHI to unauthorized individuals.

61. But for BHG's negligent conduct or breach of the above-described duties owed to Plaintiff and Class members, their PII/PHI would not have been compromised.

62. As a result of BHG's above-described wrongful actions, inaction, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiff and Class members have suffered and will suffer injury, including, but not limited to: (i) a substantial increase in the likelihood of identity theft; (ii) the compromise, publication, and theft of their PII/PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with effort attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to

their PII/PHI which remains in BHG's possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII/PHI compromised as a result of the Data Breach; and (vii) overpayment for the services that were received without adequate data security.

COUNT II
NEGLIGENCE PER SE

63. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

64. Plaintiff brings this claim against BHG Holdings, LLC on behalf of both the Nationwide Class and the XXXIV Subclass and brings this claim against BHG XXXIV, LLC on behalf of the XXXIV Subclass.

65. BHG's duties arise from, *inter alia*, the HIPAA Privacy Rule ("Standards for Privacy of Individually Identifiable Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and E, and the HIPAA Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C (collectively, "HIPAA Privacy and Security Rules").

66. BHG's duties also arise from Section 5 of the FTC Act ("FTCA"), 15 U.S.C. § 45(a)(1), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, the unfair act or practice by business, such as BHG, of failing to employ reasonable measures to protect and secure PII/PHI.

67. BHG violated HIPAA Privacy and Security Rules and Section 5 of the FTCA by failing to use reasonable measures to protect Plaintiff's and other Class members' PII/PHI and not complying with applicable industry standards. BHG's conduct was particularly unreasonable given the nature and amount of PII/PHI it obtains and stores, and the foreseeable

consequences of a data breach involving PII/PHI including, specifically, the substantial damages that would result to Plaintiff and the other Class members.

68. BHG's violation of HIPAA Privacy and Security Rules and Section 5 of the FTCA constitutes negligence per se.

69. Plaintiff and Class members are within the class of persons that HIPAA Privacy and Security Rules and Section 5 of the FTCA were intended to protect.

70. The harm occurring as a result of the Data Breach is the type of harm HIPAA Privacy and Security Rules and Section 5 of the FTCA 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 and avoid unfair practices or deceptive practices, caused the same type of harm that has been suffered by Plaintiff and Class members as a result of the Data Brach.

71. It was reasonably foreseeable to BHG that its failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII/PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems, would result in the release, disclosure, and dissemination of Plaintiff's and Class members' PII/PHI to unauthorized individuals.

72. The injury and harm that Plaintiff and the other Class members suffered was the direct and proximate result of BHG's violations of harm HIPAA Privacy and Security Rules and Section 5 of the FTCA. Plaintiff and Class members have suffered and will suffer injury, including, but not limited to: (i) a substantial increase in the likelihood of identity theft; (ii) the compromise, publication, and theft of their PII/PHI; (iii) out-of-pocket expenses associated with

the prevention, detection, and recovery from unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with effort attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI which remains in BHG's possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII/PHI compromised as a result of the Data Breach; and (vii) overpayment for the services that were received without adequate data security.

COUNT III
BREACH OF FIDUCIARY DUTY

73. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

74. Plaintiff brings this claim against BHG Holdings, LLC on behalf of both the Nationwide Class and the XXXIV Subclass and brings this claim against BHG XXXIV, LLC on behalf of the XXXIV Subclass.

75. Plaintiff and Class members gave BHG their PII/PHI in confidence, believing that BHG would protect that information. Plaintiff and Class members would not have provided BHG with this information had they known it would not be adequately protected. BHG's acceptance and storage of Plaintiff's and Class members' PII/PHI created a fiduciary relationship between BHG and Plaintiff and Class members. In light of this relationship, BHG must act primarily for the benefit of its patients and employees, which includes safeguarding and protecting Plaintiff's and Class Members' PII/PHI.

76. BHG has a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of their relationship. It breached that duty by failing to properly protect the integrity of the system containing Plaintiff's and Class Members' PII/PHI, failing

to comply with the data security guidelines set forth by HIPAA, and otherwise failing to safeguard Plaintiff's and Class members' PII/PHI that it collected.

77. As a direct and proximate result of BHG's breaches of its fiduciary duties, Plaintiff and Class members have suffered and will suffer injury, including, but not limited to: (i) a substantial increase in the likelihood of identity theft; (ii) the compromise, publication, and theft of their PII/PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with effort attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI which remains in BHG's possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII/PHI compromised as a result of the Data Breach; and (vii) overpayment for the services that were received without adequate data security.

COUNT IV
BREACH OF EXPRESS CONTRACT

78. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

79. Plaintiff brings this claim against BHG Holdings, LLC on behalf of both the Nationwide Class and the XXXIV Subclass and brings this claim against BHG XXXIV, LLC on behalf of the XXXIV Subclass.

80. Plaintiff and Class members and BHG entered into written agreements regarding the medical care, other services, and employment that BHG was to provide to Plaintiff and Class members. Plaintiff and Class members paid BHG monies or performed employment tasks for BHG and provided BHG with their PII/PHI as consideration for these

agreements. BHG's Notice of Privacy Practices is evidence that data security was a material term of these contracts.

81. Plaintiff and Class members complied with the express contract when they paid BHG, directly or through an insurance carrier, or performed employment tasks for BHG, and provided their PII/PHI to BHG.

82. BHG breached its obligations under the contracts between itself and Plaintiff and Class members by failing to implement and maintain reasonable security measures to protect and secure their PII/PHI.

83. BHG's breach of the express contracts between itself, on the one hand, and Plaintiff and Class members, on the other hand directly caused the Data Breach.

84. Plaintiff and all other Class members were damaged by BHG's breach of express contracts because: (i) they paid—directly or through their insurers—for data security protection they did not receive; (ii) they face a substantially increased risk of identity theft and medical identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (iii) their PII/PHI was improperly disclosed to unauthorized individuals; (iv) the confidentiality of their PII/PHI has been breached; (v) they were deprived of the value of their PII/PHI, for which there is a well-established national and international market; (vi) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face; and (vii) overpayment for the services that were received without adequate data security.

COUNT V
BREACH OF IMPLIED CONTRACT

85. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

86. Plaintiff brings this claim against BHG Holdings, LLC on behalf of both the Nationwide Class and the XXXIV Subclass and brings this claim against BHG XXXIV, LLC on behalf of the XXXIV Subclass.

87. In connection with receiving health care services, Plaintiff and all other Class members entered into implied contracts with BHG.

88. Pursuant to these implied contracts, Plaintiff and Class members paid money to BHG and provided BHG with their PII/PHI. In exchange, BHG agreed to, among other things, and Plaintiff understood that BHG would: (1) provide health care to Plaintiff and Class member; (2) take reasonable measures to protect the security and confidentiality of Plaintiff's and Class members' PII/PHI; and (3) protect Plaintiff's and Class members PII/PHI in compliance with federal and state laws and regulations and industry standards.

89. The protection of PII/PHI was a material term of the implied contracts between Plaintiff and Class members, on the one hand, and BHG, on the other hand. Indeed, as set forth *supra*, BHG recognized the importance of data security and the privacy of its patients' and employees' PII/PHI in its Notice of Privacy Practices. Had Plaintiff and Class members known that BHG would not adequately protect its patients', former patients', employees', and former employees' PII/PHI, they would not have received health care services or sought employment from BHG.

90. Plaintiff and Class members performed their obligations under the implied contract when they provided BHG with their PII/PHI and paid for health care services from BHG.

91. BHG breached its obligations under its implied contracts with Plaintiff and Class members in failing to implement and maintain reasonable security measures to protect

and secure their PII/PHI and in failing to implement and maintain security protocols and procedures to protect Plaintiff's and Class members' PII/PHI in a manner that complies with applicable laws, regulations, and industry standards.

92. BHG's breach of its obligations of its implied contracts with Plaintiff and Class members directly resulted in the Data Breach and the injuries that Plaintiff and all other Class members have suffered from the Data Breach.

93. Plaintiff and all other Class members were damaged by BHG's breach of implied contracts because: (i) they paid—directly or through their insurers—for data security protection they did not receive; (ii) they face a substantially increased risk of identity theft and medical identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (iii) their PII/PHI was improperly disclosed to unauthorized individuals; (iv) the confidentiality of their PII/PHI has been breached; (v) they were deprived of the value of their PII/PHI, for which there is a well-established national and international market; (vi) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face; and (vii) overpayment for the services that were received without adequate data security.

COUNT VI
UNJUST ENRICHMENT

94. Plaintiff realleges and incorporates by reference paragraphs 1–51 as if fully set forth herein.

95. Plaintiff brings this claim against BHG Holdings, LLC on behalf of both the Nationwide Class and the XXXIV Subclass and brings this claim against BHG XXXIV, LLC on behalf of the XXXIV Subclass.

96. This claim is pleaded in the alternative to the breach of express contract and breach of implied contract claims.

97. Plaintiff and Class members conferred a monetary benefit upon BHG in the form of monies paid for health care services, or in the form of employment.

98. BHG accepted or had knowledge of the benefits conferred upon it by Plaintiff and Class Members. BHG also benefitted from the receipt of Plaintiff's and Class members' PII/PHI, as this was used to facilitate the billing services.

99. As a result of BHG's conduct, Plaintiff and Class members suffered actual damages in an amount equal to the difference in value between their payments made with reasonable data privacy and security practices and procedures that Plaintiff and Class members paid for, and those payments without reasonable data privacy and security practices and procedures that they received.

100. BHG should not be permitted to retain the money belonging to Plaintiff and Class members because BHG failed to adequately implement the data privacy and security procedures for itself that Plaintiff and Class members paid for and that were otherwise mandated by federal, state, and local laws and industry standards.

101. BHG should be compelled to provide for the benefit of Plaintiff and Class members all unlawful proceeds received by it as a result of the conduct and Data Breach alleged herein.

PRAYER FOR RELIEF

Plaintiff, individually and on behalf of all other members of the Class, respectfully requests that the Court enter judgment in her favor and against BHG as follows:

A. Certifying the Class as requested herein, designating Plaintiff as Class representative, and appointing Plaintiff's counsel as Class Counsel;

B. Awarding Plaintiff and the Class appropriate monetary relief, including actual damages, statutory damages, punitive damages, restitution, and disgorgement;

C. Awarding Plaintiff and the Class equitable, injunctive, and declaratory relief, as may be appropriate. Plaintiff, on behalf of herself and the Class, seeks appropriate injunctive relief designed to prevent BHG from experiencing another data breach by adopting and implementing best data security practices to safeguard PII/PHI and to provide or extend credit monitoring services and similar services to protect against all types of identity theft and medical identity theft;

D. Awarding Plaintiff and the Class pre-judgment and post-judgment interest to the maximum extent allowable;

E. Awarding Plaintiff and the Class reasonable attorneys' fees, costs, and expenses, as allowable; and

F. Awarding Plaintiff and the Class such other favorable relief as allowable under law.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury of all claims in this Class Action Complaint so triable.

Dated: September 2, 2022

Respectfully submitted,

/s/ Mark K. Gray

Mark K. Gray
Matthew L. White
Gray & White, PLLC
2301 River Road #300
Louisville, KY 40206
Tel: 502-210-8942
Fax: 502-618-4059
mgray@grayandwhitelaw.com
mwhite@grayandwhitelaw.com

Ben Barnow (pro hac vice forthcoming)
Anthony L. Parkhill (pro hac vice forthcoming)
Riley W. Prince (pro hac vice forthcoming)
Barnow and Associates, P.C.
205 West Randolph Street, Ste. 1630
Chicago, IL 60606
Tel: 312-621-2000
Fax: 312-641-5504
b.barnow@barnowlaw.com
aparkhill@barnowlaw.com
rprince@barnowlaw.com

ClassAction.org

This complaint is part of ClassAction.org's searchable class action lawsuit database and can be found in this post: Behavioral Health Group Facing Class Action Over December 2021 Data Breach