UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF KENTUCKY
LEXINGTON DIVISION

VIRGINIA HILEY and ANTHONY LEROY WHITE, individually and on behalf of all others similarly situated,

Plaintiffs,

v.

CORRECTCARE INTEGRATED HEALTH, LLC,

Defendant.

CASE NO: 5:22-cv-00319-DCR

JURY DEMAND

CLASS ACTION

FIRST AMENDED CLASS ACTION COMPLAINT

Plaintiffs Virginia Hiley and Anthony Leroy White("Plaintiffs"), individually and on behalf of all others similarly situated, bring this Amended Class Action Complaint and allege the following against Defendant CorrectCare Integrated Health, LLC ("CorrectCare" or "Defendant"), based upon personal knowledge with respect to Plaintiffs and upon information and belief derived from, among other things, investigation of counsel and review of public documents as to all other matters:

NATURE OF THE ACTION

1. This class action arises out of the recent data breach (the "Data Breach") involving CorrectCare, which collected and stored certain Protected Health Information ("PHI") and Personal Identifying Information ("PII") of the Plaintiffs and the putative Class Members, all of whom have PHI and PII on CorrectCare servers.

2. According to CorrectCare, the PHI compromised in the Data Breach "potentially expos[ed]" files that contained highly-sensitive information, including, but not limited to: names, dates of birth, health information such as diagnosis codes and/or Cognitive Processing Therapy treatment codes ("CPT"), treatment providers, and dates of treatment, and potentially Social Security Numbers.[1]

3. In addition, CorrectCare's notification letters stated TIN (Taxpayer Identification Number) may have been exposed.

4. Social Security numbers and TINs are particularly valuable to criminals. This information can be sold and traded on the dark web black market. The loss of a Social Security number is especially troubling because it cannot be easily changed and can be misused in a range of nefarious activities, such as filing fraudulent tax returns to steal tax refund payments, opening new accounts to take out loans, and other forms of identity theft.

5. The Data Breach was a direct result of CorrectCare's failure to implement adequate and reasonable cybersecurity procedures and protocols necessary to protect consumers' PHI and PII. Inexplicitly, the Defendant has acknowledged that it first became aware of the exposure of information stores on its web server to the public on July 6, 2022, that the directories may have been exposed as early as January 2, 2022, but it has only recently begun contacting Class Members.[2]

[1] *See* "Mediko, Inc. Provides Notice of Data Privacy Event." https://www.prnewswire.com/news-releases/mediko-inc-provides-notice-of-data-privacy-event-301663843.html (last accessed December 5, 2022).
[2] *Id.*

6. According to state officials in Louisiana, the Data Breach has affected 80,000 individuals who have interacted with the Louisiana Department of Public Safety and Corrections.[3] Since the Breach, CorrectCare has confirmed with the Department of Health and Human Services' Office for Civil Rights that at a minimum, the PHI of more than 590,000 individuals had been exposed.[4]

7. Plaintiffs bring this class action lawsuit on behalf of themselves and all those similarly situated to address Defendant's inadequate safeguarding of Class Members' PHI and PII that they collected and maintained, and for failing to provide timely and adequate notice to Plaintiffs and other Class Members that their information was unsecured and left open to the unauthorized access of any unknown third party.

PARTIES

8. Plaintiff Virginia Hiley is an adult individual and citizen of Louisiana.

9. Plaintiff Hiley's PHI and PII was stored and handled by CorrectCare. Plaintiff Hiley was formerly incarcerated at different facilities in Louisiana. During these time periods, she received medical treatment, the claims of which were processed through CorrectCare. On December 2, 2022, she was notified by CorrectCare via letter dated November 28, 2022 of the Data Breach and of the impact to her PHI.

[3] "Important information on Data Breach." https://doc.louisiana.gov/data-breach-louisiana-doc/#:~:text=is%20potentially%20affected%3F-,The%20exposure%20of%20two%20file%20directories%20on%20a%20single%20server,%2C%20and%20July%207%2C%202022. (last accessed January 17, 2023).

[4] "Update: CorrectCare Integrated Health Data Breach Affects Hundreds of Thousands of Inmates." https://www.hipaajournal.com/correctcare-integrated-health-data-breach-affects-thousands-of-inmates/ (last accessed January 17, 2023).

10. Since the Data Breach, Plaintiff Hiley has had numerous accounts breached, including her account with Amazon.com and a relative's Google account. She has also received numerous phishing and scam calls since the Breach, including calls from apparent "creditors" telling her she owed them money. Given the highly-sensitive nature of the information stolen, Plaintiff Hiley remains at a substantial and imminent risk of future harm.

11. Plaintiff Anthony Leroy White is an adult and a citizen of Georgia.

12. Plaintiff White's PHI and PII was stored and handled by CorrectCare. Plaintiff White has been incarcerated at Dodge State Prison in the state of Georgia. While incarcerated, he received medical treatment, the claims of which were processed through CorrectCare. In December 2022, he received a letter dated November 28, 2022 from CorrectCare notifying him of the Data Breach and the exposure of his PHI and PII.

13. Defendant White has had to spend time monitoring his accounts to detect suspicious and fraudulent activity to mitigate against potential harm. Mr. White monitors his accounts from prison which is difficult because computer access is limited, causing him stress and anxiety. Given the highly-sensitive nature of the information stolen, Plaintiff White remains at a substantial and imminent risk of future harm.

14. As a result of Defendant's conduct, Plaintiffs suffered actual damages including, without limitation, time and expenses related to monitoring their financial accounts for fraudulent activity, facing an increased and imminent risk of fraud and identity theft, the lost value of their personal information, and other economic and non-economic harm. Plaintiffs and Class Members will now be forced to expend additional time to review their credit reports and monitor their financial accounts and medical records for fraud or identify theft – particularly since the compromised information may include Social Security numbers.

15. Defendant CorrectCare is a limited liability company with a principal place of business and headquarters in Fayette County, with an address at 1218 South Broadway, Suite 250, Lexington, Kentucky. According to the Kentucky Secretary of State, the three members of the limited liability company (Tucker J. Stein, Thomas J. Georgouses and Justin Tran) all maintain a place of business at 621 Santa Fe, Fresno, CA 93721.

JURISDICTION AND VENUE

16. This Court has subject matter jurisdiction over this controversy pursuant to The Class Action Fairness Act of 2005 ("CAFA"). 28 U.S.C. § 1332(d)(2).

17. The amount in controversy in this class action exceeds $5,000,000, exclusive of interest and costs, and there are numerous Class members who are citizens of states other than Defendant's state of citizenship. Specifically, the Plaintiff Hiley is a citizen of Louisiana, Plaintiff White is a citizen of Georgia, and the Defendant limited liability company is deemed a citizen of Kentucky and California, as Defendant's principal place of business in in Kentucky and all of all its members are based in California and are citizens of California.

18. This Court has personal jurisdiction over Defendant because it is authorized to and does conduct substantial business in this District through its headquarter and offices, and because Defendant's principal place of business is in this District.

19. Venue is proper under 28 U.S.C. §1391(b) because the cause of action upon which the complaint is based arose in Lexington, KY, which is in the Eastern District of Kentucky, and because a substantial part of the events and omissions giving rise to this action occurred in this District – the place where Defendant's computer systems and networks are maintained and were breached.

COMMON FACTUAL ALLEGATIONS

20. Plaintiffs and the proposed Class are individuals who had their PHI and PII handled by CorrectCare. CorrectCare is a medical claims processor servicing corrections facilities.[5]

21. As noted above, Plaintiffs bring this class action against Defendant for Defendant's failure to properly secure and safeguard Protected Health Information as defined by the Health Insurance Information Portability and Accountability Act ("HIPAA"), medical information, and other Personally Identifiable Information, for failing to comply with industry standards to protect and safeguard that information, and for failing to provide timely and adequate notice to Plaintiffs and other members of the class that such information had been compromised.

CorrectCare's Unsecure Data Management and Disclosure of Data Breach

22. Plaintiffs and Class Members provided their PHI and PII to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

23. Plaintiffs and Class Member's PHI and PII was provided to Defendant in conjunction with the type of work Defendant does within the healthcare industry, specifically processing medical claims in the correctional setting.

24. However, CorrectCare failed to secure the PHI and PII of the individuals that provided it with this sensitive information.

25. CorrectCare's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches preceding the date they disclosed the incident.

[5] "CorrectCare Integrated Health." https://www.corrections.direct/united-states/lexington/corrections/correctcare-integrated-health-3755 (last accessed January 17, 2023).

26. According to PR Newswire, CorrectCare first discovered, on July 6, 2022, "that two file directories on its web server had been inadvertently exposed to the public internet."[6]

27. After conducting an initial investigation, CorrectCare "determined patient information contained in these file directories may have been exposed as early as January 22, 2022."[7] CorrectCare noted that the patient information affected "included name, date of birth, and limited health information, such as a diagnosis code and/or CPT code, treatment provider, and dates of treatment, and may have included Social Security numbers."[8]

28. Despite first becoming aware of the existence of the Data Breach on July 6, 2022 – and conducting "promptly" an investigation "with the assistance of third-party cyber security specialists" – CorrectCare waited until after Thanksgiving, in November, to begin notifying individuals that their information was compromised.

29. The data implicated in CorrectCare's breach goes far beyond the window in which it was allegedly accessed, as records dating as far back as 2013 – records ten years old – were allegedly accessed by unauthorized parties."[9]

The Data Breach was a Foreseeable Risk of which Defendant was on Notice

30. Cyberattacks against the healthcare industry have been common for over ten years with the Federal Bureau of Investigation ("FBI") warning as early as 2011 that cybercriminals were "advancing their abilities to attack a system remotely" and "[o]nce a system is compromised,

[6] *See* n. 1.
[7] *Id.*
[8] *Id.*
[9] https://doc.louisiana.gov/data-breach-louisiana-doc/ (last accessed January 16, 2023).

cyber criminals will use their accesses to obtain PII." The FBI further warned that that "the increasing sophistication of cyber criminals will no doubt lead to an escalation in cybercrime."[10]

31. Cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals… because they often have lesser IT defenses and a high incentive to regain access to their data quickly.[11]

32. In fact, according to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in the past year.[12]

33. CorrectCare was on notice that the FBI has recently been concerned about data security in the healthcare industry. In August 2014, after a cyberattack on Community Health Systems, Inc., the FBI warned companies within the healthcare industry that hackers were targeting them. The warning stated that "[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining the Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII)."[13]

---

[10] Gordon M. Snow, *Statement before the House Financial Services Committee, Subcommittee on Financial Institutions and Consumer Credit*, FBI (Sept. 14, 2011), https://archives.fbi.gov/archives/news/testimony/cyber-security-threats-to-the-financial-sector (last visited November 30, 2022).

[11] Ben Kochman, *FBI, Secret Service Warn of Targeted Ransomware*, LAW360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware (last visited November 30, 2022).

[12] *See* Maria Henriquez, *Iowa City Hospital Suffers Phishing Attack,* SECURITY MAGAZINE (Nov. 23, 2020), https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing-attack (last visited November 30, 2022).

[13] Jim Finkle, *FBI Warns Healthcare Firms that they are Targeted by Hackers*, REUTERS (Aug. 2014), https://www.reuters.com/article/us-cybersecurity-healthcare-fbi/fbi-warns-healthcare-firms-they-are-targeted-by-hackers-idUSKBN0GK24U20140820 (last visited November 30, 2022).

34. The American Medical Association ("AMA") has also warned healthcare companies about the importance of protecting their patients' confidential information:

> Cybersecurity is not just a technical issue; it's a patient safety issue. AMA research has revealed that 83% of physicians work in a practice that has experienced some kind of cyberattack. Unfortunately, practices are learning that cyberattacks not only threaten the privacy and security of patients' health and financial information, but also patient access to care.[14]

35. As implied by the above AMA quote, stolen PHI can be used to interrupt important medical services. This is an imminent and certainly impending risk for Plaintiffs and Class Members.

36. Cyber criminals seek out PHI at a greater rate than other sources of personal information. In a 2022 report, the healthcare compliance company Proetus found that there were 905 medical data breaches in 2021, leaving over 50 million patient records exposed for 700 of the 2021 incidents. This is an increase from the 758 medical data breaches that Protenus compiled in 2020.[15]

37. The healthcare sector suffered about 337 breaches in the first half of 2022 alone, according to Fortified Health Security's mid-year report released in July. The percentage of healthcare breaches attributed to malicious activity rose more than 5 percentage points in the first six months of 2022 to account for nearly 80 percent of all reported incidents.[16]

---

[14] Andis Robeznieks, *Cybersecurity: Ransomware attacks shut down clinics, hospitals*, AM. MED. ASS'N (Oct. 4, 2019), https://www.ama-assn.org/practice-management/sustainability/cybersecurity-ransomware-attacks-shut-down-clinics-hospitals (last visited November 30, 2022).

[15] *2022 Breach Barometer*, PROTENUS, https://www.protenus.com/breach-barometer-report (last accessed on January 16, 2023).

[16] Jill McKeon, *Health Sector Suffered 337 Healthcare Data Breaches in First Half of Year*, Cybersecurity News (July 19, 2022), https://healthitsecurity.com/news/health-sector-suffered-337-healthcare-data-breaches-in-first-half-of-year (last visited January 16, 2023).

38. Further, a 2022 report released by IBM Security states that for 12 consecutive years the healthcare industry has had the highest average cost of a data breach and as of 2022 healthcare data breach costs have hit a new record high.[17]

39. Before the Data Breach, Defendant knew or should have known that there was a foreseeable risk that Plaintiffs' and Class Members' PHI could be accessed, exfiltrated, and published as the result of a cyberattack. Notably, data breaches are prevalent in today's society and especially in the health industry, therefore making the risk of experiencing a data breach entirely foreseeable to CorrectCare.

CorrectCare Owed a Duty to Plaintiffs and Class Members to Properly Secure Their PHI

40. At all relevant times, CorrectCare had a duty to Plaintiffs and Class Members to properly secure their PII, encrypt and maintain such information using industry standard methods, train its employees, utilize available technology to defend its systems from invasion, act reasonably to prevent foreseeable harm to Plaintiffs and Class Members, and to promptly notify Plaintiffs and Class Members when CorrectCare became aware that their PHI and PII may have been compromised.

41. CorrectCare's duty to use reasonable security measures arose as a result of the special relationship that existed between CorrectCare and the Plaintiffs and the Class Members. The special relationship arose because Plaintiffs and the Class Members entrusted CorrectCare with their PHI and PII as a condition of receiving medical services for themselves.

42. CorrectCare had the resources necessary to prevent the Data Breach but neglected to adequately invest in security measures, despite its obligation to protect such information.

[17] *Cost of a Data Breach Report 2022*, IBM Security, https://www.ibm.com/downloads/cas/3R8N1DZJ (last visited January 16, 2023).

Accordingly, CorrectCare breached its common law, statutory, and other duties owed to Plaintiffs and Class Members.

43. CorrectCare failed to employ security standards commonly accepted among businesses and required by security standards of businesses that store PHI and PII and use the internet.

FTC Guidelines Prohibit Unfair or Deceptive Acts

44. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[18] 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."[19]

45. CorrectCare is prohibited by the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTC Act") from engaging in "unfair or deceptive acts or practices in or affecting commerce." The FTC has concluded that a company's failure to maintain reasonable and appropriate data security for individuals' sensitive personal information is an "unfair practice" in violation of the FTC Act.

[18] 17 C.F.R. § 248.201 (2013).
[19] *Id.*

46. The FTC has promulgated numerous guides for businesses that 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.[20]

47. The FTC provided cybersecurity guidelines for businesses, advising that businesses should protect personal customer information, properly dispose of personal information that is no longer needed, encrypt information stored on networks, understand their network's vulnerabilities, and implement policies to correct any security problems.[21]

48. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to private 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.[22]

49. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential customer data as an unfair act or practice prohibited by Section 5 of the FTC Act. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

50. CorrectCare failed to properly implement basic data security practices. CorrectCare's failure to employ reasonable and appropriate measures to protect against

[20] https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited Jan. 16, 2023).
[21] https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Jan. 16, 2023).
[22] *Id.*

unauthorized access to Plaintiffs' and Class Members' PHI and PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act.

51. CorrectCare was at all times fully aware of its obligations to protect the PHI and PII of Plaintiffs and Class Members because CorrectCare collected PHI and PII and stored such information for analysis and for pecuniary gain. CorrectCare was also aware of the significant repercussions that would result from its failure to do so.

52. The ramifications of CorrectCare's failure to keep Plaintiffs' and Class Members' PHI and PII secure are long lasting and severe. Once PHI and PII is stolen, particularly Social Security numbers and TINs as here, fraudulent use of that information and damage to victims is likely to continue for years.

HIPAA Standards & Violations

53. Upon information and belief, CorrectCare failed to create, maintain, and/or comply with a written cybersecurity program that incorporated physical, technical, and administrative safeguards for the protection of its Plaintiffs' and Class Members' PHI in compliance with industry recognized cybersecurity framework and HIPAA.

54. The security failures include but are not limited to:

a. Failing to maintain an adequate security system to prevent data loss;

b. Failing to implement policies and procedures that limit use and disclosure PHI;

c. Failing to mitigate the risks of data breach and loss of data;

d. Failing to ensure the confidentiality and integrity of electronic PHI that Defendant receives, maintains, and transmits in violation of 45 C.F.R. 164. 306(a)(1);

e. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access to only those

persons or software programs that have been granted access in violation of 45 C.F.R. 164.312(a)(1);

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

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

h. Failing to ensure compliance with HIPAA security standards by their workforce or agents in violation of 45 C.F.R 164.306(a)(94);

i. Failing to effectively train all members of its workforce and its agents on the policies and procedures with respect to PHI as necessary to maintain the security of PHI in violation of 45 C.F.R. 164.530(b) and 45 C.F.R. 164.308(a)(5);

j. Failing to design and implement and enforce policies and procedures to establish administrative safeguards to reasonably safeguard PHI in compliance with 45 C.F.R. 164.530(c); and,

k. Releasing, transferring, allowing access to, and divulging protected PHI to unauthorized criminal third parties.

Plaintiffs and the Class Have Suffered Injury as a Result of CorrectCare's Failure to Employ Adequate Data Security

55. As a result of Defendant's failure to implement and follow even the most basic security procedures, Plaintiffs' and Class Members' PHI and PII have been and are now in the hands of unauthorized individuals, which may include thieves, unknown criminals, banks, credit companies, and other potentially hostile individuals. Plaintiffs and other Class Members now face an increased risk of identity theft, particularly due to the potential dissemination of their Social Security Number and other impacted information, and will continue to spend, significant time and money to protect themselves due to Defendant's Data Breach.

56. Plaintiffs and other class members have had their most personal, sensitive and PHI and PII disseminated to the public at large and have experienced and will continue to experience emotional pain and mental anguish and embarrassment.

57. Plaintiffs and Class members face an increased risk of identity theft, phishing attacks, and related cybercrimes because of the Data Breach. Those impacted are under heightened and prolonged anxiety, as they will be at risk for falling victim for cybercrimes for years to come.

58. PII/PHI is a valuable property right.[23] The value of PII/PHI as a commodity is measurable.[24] "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."[25] American companies are estimated to have spent over $19 billion on acquiring personal data of consumers in 2018.[26] 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.

59. As a result of its real value and the recent large-scale data breaches, identity thieves and cyber criminals have openly posted credit card numbers, Social Security numbers, 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

---

[23] *See* Marc van Lieshout, *The Value of Personal Data*, 457 IFIP ADVANCES IN INFORMATION AND COMMUNICATION TECHNOLOGY 26 (May 2015), https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible...") (last visited January 17, 2023).

[24] *See* Robert Lowes, *Stolen EHR [Electronic Health Record] Charts Sell for $50 Each on Black Market*, MEDSCAPE (Apr. 28, 2014), http://www.medscape.com/viewarticle/824192 (last visited January 17, 2023).

[25] *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD 4 (Apr. 2, 2013), https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en. (last visited on January 17, 2023).

[26] *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*, INTERACTIVE ADVERTISING BUREAU (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/ (last visited January 17, 2023).

the Data Breach, can be aggregated and become more valuable to thieves and more damaging to victims.

60. PHI is particularly valuable and has been referred to as a "treasure trove for criminals."[27] A cybercriminal who steals a person's PHI can end up with as many as "seven to 10 personal identifying characteristics of an individual."[28] A study by Experian found that the "average total cost" of medical identity theft is "about $20,000" per incident, and that a majority of victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[29]

61. Personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[30] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[31] 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.[32] Criminals can also purchase access to

---

[27] *See* Andrew Steger, *What Happens to Stolen Healthcare Data?*, HEALTHTECH MAGAZINE (Oct. 30, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon (quoting Tom Kellermann, Chief Cybersecurity Officer, Carbon Black, stating "Health information is a treasure trove for criminals.") (last visited January 17, 2023).

[28] *Id.*

[29] Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (Mar. 3, 2010, 5:00 AM), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims (last visited January 17, 2023).

[30] Anita George, *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends (Oct. 16, 2019), https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last visited January 17, 2023).

[31] Brian Stack, *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian (Dec. 6, 2017), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited January 17, 2023).

[32] Adam Greenberg, *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 (last visited January 17, 2023).

entire company data breaches from $900 to $4,500.[33] 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.[34]

62. Criminals can use stolen PII/PHI to extort a financial payment by "leveraging details specific to a disease or terminal illness."[35] 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."[36]

63. Consumers place a high value on the privacy of that data. 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."[37]

64. 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.

---

[33] *In the Dark*, VPNOverview.com, 2019, https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed on January 17, 2023).

[34] *See Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain*, FBI CYBER DIVISION (Apr. 8, 2014), https://nsarchive.gwu.edu/document/18867-national-security-archive-department-justice. (last accessed January 17, 2023).

[35] *See* n.44, *supra*.

[36] *Id.*

[37] 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. (last accessed January 17, 2023).

65. Plaintiffs and members of the Class, as a whole, must immediately devote time, energy, and money to: 1) closely monitor their medical statements, bills, records, and credit and financial accounts; 2) change login and password information on any sensitive account even more frequently than they already do; 3) more carefully screen and scrutinize phone calls, emails, and other communications to ensure that they are not being targeted in a social engineering or spear phishing attack; and 4) search for suitable identity theft protection and credit monitoring services, and pay to procure them.

66. Once PHI and PII are exposed, there is virtually no way to ensure that the exposed information has been fully recovered or contained against future misuse. For this reason, Plaintiffs and Class Members will need to maintain these heightened measures for years, and possibly their entire lives, as a result of CorrectCare's conduct. Further, the value of Plaintiffs' and Class Members' PHI and PII have been diminished by their exposure in the Data Breach.

67. As a result of CorrectCare's data security failures, Plaintiffs and Class Members are at substantial risk of suffering identity theft and fraud or misuse of their PHI and PII.

68. Plaintiffs and Class Members suffered actual injury from having PHI and PII compromised as a result of CorrectCare's negligent data management and resulting Data Breach including, but not limited to (a) damage to and diminution in the value of their PHI and PII, a form of property that Defendant obtained from Plaintiffs and Class Members; (b) violation of their privacy rights; and (c) present and increased risk arising from the identity theft and fraud.

69. For the reasons mentioned above, CorrectCare's conduct, which allowed the Data Breach to occur, caused Plaintiffs and Class Members these significant injuries and harm.

70. Plaintiffs bring this class action against Defendant for Defendant's failure to properly secure and safeguard PHI and PII and for failing to provide timely, accurate, and adequate notice to Plaintiffs and Class Members that their PHI and PII have been compromised.

71. Plaintiffs, individually and on behalf of all other similarly situated individuals, allege claims in negligence, negligence per se, breach of implied contract, breach of fiduciary duty, and unjust enrichment.

CLASS ACTION ALLEGATIONS

72. Plaintiffs brings this action on behalf of themselves and on behalf of all other persons similarly situated.

73. Plaintiffs propose the following Class definition, subject to amendment as appropriate:

> All persons whose Private Health Information and Personal Identifying Information were compromised as a result of the Data Breach discovered by CorrectCare on or around June 6, 2022 (the "Class").

74. Excluded from the Class are Defendant's officers and directors, and any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class are Members of the judiciary to whom this case is assigned, their families and Members of their staff.

75. Plaintiffs reserve the right to amend or modify the class definitions with greater specificity or division after having had an opportunity to conduct discovery. The proposed Classes meet the criteria for certification under Rule 23(a), 23(b)(2), 23(b)(3), and 23(c)(4).

76. Numerosity. The Members of the Class are so numerous that joinder of all of them is impracticable. As noted above, the data breach affected almost 500,000 individuals.

77. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiffs' and Class Members' PHI and PII;

b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

d. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether Defendant owed a duty to Class Members to safeguard their PHI and PII;

f. Whether Defendant breached its duty to Class Members to safeguard their PHI and PII;

g. Whether computer hackers obtained Class Members' PHI and PII in the Data Breach;

h. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

i. Whether Plaintiffs and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

j. Whether Defendant's conduct was negligent;

k. Whether Defendant's conduct was per se negligent;

l. Whether Defendant's acts, inactions, and practices complained of herein amount to acts of intrusion upon seclusion under the law;

m. Whether Defendant was unjustly enriched;

n. Whether Defendant failed to provide notice of the Data Breach in a timely manner; and

o. Whether Plaintiffs and Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

78. Typicality. Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' PHI and PII, like that of every other Class Member, was compromised in the Data Breach.

79. Adequacy of Representation. Plaintiffs will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiffs' Counsel are competent and experienced in litigating class actions, including data privacy litigation of this kind.

80. Predominance. Defendant has engaged in a common course of conduct toward Plaintiffs and Class Members, in that all the Plaintiffs' and Class Members' data was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

81. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class

Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class member.

82. Defendant has acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

83. Likewise, particular issues 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 Defendant failed to timely notify the public of the Data Breach;

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

c. Whether Defendant's security measures to protect their 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 consumer PHI and PII; and

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

84. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to Class Members' names and addresses affected by the Data Breach. In fact, Class Members have already been preliminarily identified and sent notice of the Data Breach by Defendant.

CAUSES OF ACTION

First Count
Negligence
(On Behalf of Plaintiffs and Class Members)

85. Plaintiffs re-allege and incorporate the paragraphs 1 – 84 above as if fully set forth herein.

86. CorrectCare required Plaintiffs and Class Members to submit non-public personal information in order to obtain healthcare/medical services.

87. By collecting and storing this data in CorrectCare's computer property, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard their computer property—and Class Members' PHI and PII held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which it could detect a breach of their security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a Data Breach.

88. Defendant owed a duty of care to Plaintiffs and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure

that its systems and networks, and the personnel responsible for them, adequately protected the PHI.

89. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant CorrectCare and its patients, which is recognized by laws and regulations including but not limited to HIPAA, as well as common law. Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a Data Breach or data breach.

90. Defendant's duty to use reasonable security measures under HIPAA required Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). Some or all of the healthcare, medical, and/or medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

91. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

92. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential PHI and PII.

93. Defendant breached its duties, and thus were negligent, by failing to use reasonable measures to protect Class Members' PHI and PII. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' PHI and PII;

b. Failing to adequately monitor the security of their networks and systems;

c. Failure to periodically ensure that their email system had plans in place to maintain reasonable data security safeguards;

d. Allowing unauthorized access to Class Members' PHI and PII;

e. Failing to detect in a timely manner that Class Members' PHI and PII had been compromised;

f. Failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages;

g. Failing to secure its web servers from unauthorized and public access; and

94. It was foreseeable that Defendant's failure to use reasonable measures to protect Plaintiffs' and Class Members' PHI and PII would result in injury to them. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the healthcare industry.

95. It was therefore foreseeable that the failure to adequately safeguard Plaintiffs' and Class Members' PHI and PII would result in one or more types of injuries to them.

96. Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

97. Defendant's negligent conduct is ongoing, in that it still holds the PHI and PII of Plaintiffs and Class Members in an unsafe and unsecure manner.

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

Second Count
Breach of Implied Contract
(On Behalf of Plaintiffs and Class Members)

99. Plaintiffs re-allege paragraphs 1-84 as if fully set forth herein.

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

101. Defendant CorrectCare solicited, offered, and invited Class Members to provide their PHI and PII as part of Defendant's regular business practices. Plaintiffs and Class Members accepted Defendant's offers and provided their PHI and PII to Defendant.

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

103. Plaintiffs and Class Members paid money to Defendant with the reasonable belief and expectation that Defendant would use part of its earnings to obtain adequate data security. Defendant failed to do so.

104. In accepting Plaintiffs' and Class Members' PHI and PII and payment for services, Plaintiffs and the Class Members entered into an implied contract with CorrectCare whereby CorrectCare became obligated to reasonably safeguard Plaintiffs' and the Class Members' PHI and PII.

105. Plaintiffs and Class Members would not have entrusted their PHI and PII to Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure.

106. Plaintiffs and Class Members would not have entrusted their PHI and PII to Defendant in the absence of their implied promise to monitor their computer systems and networks to ensure that it adopted reasonable data security measures.

107. Plaintiffs and Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

108. Defendant breached its implied contracts with Class Members by failing to safeguard and protect their PHI and PII.

109. As a direct and proximate result of Defendant's breach of the implied contracts, Class Members sustained damages as alleged herein, including the loss of the benefit of the bargain.

110. Plaintiffs and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

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

Third Count
Negligence *Per Se*
(On Behalf of Plaintiffs and All Class Members)

112. Plaintiffs re-allege paragraphs 1-84 as if fully set forth herein.

113. Pursuant to the Federal Trade Commission Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' PHI and PII.

114. Pursuant to HIPAA, 42 U.S.C. § 1302d, et seq., Defendant had a duty to implement reasonable safeguards to protect Plaintiffs' and Class Members' PHI.

115. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by companies such as CorrectCare for failing to use reasonable measures to protect PHI and PII. Various FTC publications and orders also form the basis of CorrectCare's duty.

116. Defendant CorrectCare violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and PHI and not complying with the industry standards. Defendant CorrectCare's 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.

117. Plaintiffs and Class Members are consumers within the class of persons Section 5 of the FTC Act was intended to protect.

118. Pursuant to HIPAA, Defendant had a duty to render the electronic PHI they maintained unusable, unreadable, or indecipherable to unauthorized individuals, as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key." *See* definition of encryption at 45 C.F.R. § 164.304.

119. Defendant breached its duties to Plaintiffs and Class Members under the Federal Trade Commission Act and HIPAA by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' PHI and PII.

120. Defendant's failure to comply with applicable laws and regulations constitutes negligence *per se*.

121. But for Defendant's wrongful and negligent breach of their duties owed to Plaintiffs and Class Members, Plaintiffs and Class Members would not have been injured.

122. The injury and harm suffered by Plaintiffs and Class Members was the reasonably foreseeable result of Defendant's breach of their duties. Defendant knew or should have known that they failing to meet its duties, and that Defendant's breach would cause Plaintiffs and Class Members to experience the foreseeable harms associated with the exposure of their PHI and PII.

123. As a direct and proximate result of Defendant's negligent conduct, Plaintiffs and Class Members have suffered injury and are entitled to compensatory, consequential, and punitive damages in an amount to be proven at trial.

Fourth Count
Breach of Fiduciary Duty
(On Behalf of Plaintiffs and Class Members)

124. Plaintiffs re-allege paragraphs 1-84 as if fully set forth herein.

125. In light of the confidential medical relationship between Defendant CorrectCare and Plaintiffs and Class Members, whereby Defendant became guardian of Plaintiffs' and Class Members' PHI and PII, Defendant became a fiduciary by its undertaking and guardianship of the PHI and PII, to act primarily for Plaintiffs and Class Members, (1) for the safeguarding of Plaintiffs' and Class Members' PHI and PII; (2) to timely notify Plaintiffs and Class Members of a Data Breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendant did and does store.

126. Defendant has a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of CorrectCare's relationship with its patients and former patients, in particular, to keep secure their PHI and PII.

127. Defendant breached its fiduciary duties to Plaintiffs and Class Members by failing to diligently discovery, investigate, and give notice of the Data Breach in a reasonable and practicable period of time.

128. Defendant breached its fiduciary duties to Plaintiffs and Class Members by failing to encrypt and otherwise protect the integrity of the systems containing Plaintiffs' and Class Members' PHI and PII.

129. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by failing to timely notify and/or warn Plaintiffs and Class Members of the Data Breach.

130. Defendant breached its fiduciary duties to Plaintiffs and Class Members by otherwise failing to safeguard Plaintiffs' and Class Members' PHI and PII.

131. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their PHI and PII; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their PHI and PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PHI and PII in

their continued possession; (vi) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members; and (vii) the diminished value of Defendant's services they received.

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

Fifth Count
Intrusion Upon Seclusion / Invasion of Privacy
(On Behalf of Plaintiffs and All Class Members)

133. Plaintiffs re-allege paragraphs 1-84 as if fully set forth herein.

134. Plaintiffs and Class Members had a reasonable expectation of privacy in the PHI and PII Defendant mishandled.

135. Defendant owed a duty to Plaintiffs and Class Members to keep this information confidential.

136. Defendant's conduct as alleged above intruded upon Plaintiffs' and Class Members' seclusion under common law.

137. By intentionally failing to keep Plaintiffs' and Class Members' PHI and PII safe, and by intentionally misusing and/or disclosing said information to unauthorized parties for unauthorized use, Defendant intentionally invaded Plaintiffs' and Class Members' privacy by:

a. Intentionally and substantially intruding into Plaintiffs' and Class Members' private affairs in a manner that identifies Plaintiffs and Class Members and that would be highly offensive and objectionable to an ordinary person; and

b. Intentionally publicizing private facts about Plaintiffs and Class Members, which is highly offensive and objectionable to an ordinary person; and

c. Intentionally causing anguish or suffering to Plaintiffs and Class Members.

138. Defendant knew that an ordinary person in Plaintiffs' or Class Members' position would consider Defendant's intentional actions highly offensive and objectionable.

139. Defendant invaded Plaintiffs' and Class Members' right to privacy and intruded into Plaintiffs' and Class Members' private affairs by intentionally misusing and/or disclosing their PHI without their informed, voluntary, affirmative, and clear consent.

140. Defendant intentionally concealed from and delayed reporting to Plaintiffs and Class Members a security incident that misused and/or disclosed their PHI and PII without their informed, voluntary, affirmative, and clear consent.

141. The conduct described above was at or directed at Plaintiffs and the Class Members.

142. As a proximate result of such intentional misuse and disclosures, Plaintiffs' and Class Members' reasonable expectations of privacy in their PHI and PII was unduly frustrated and thwarted. Defendant's conduct amounted to a substantial and serious invasion of Plaintiffs' and Class Members' protected privacy interests causing anguish and suffering such that an ordinary person would consider Defendant's intentional actions or inaction highly offensive and objectionable.

143. In failing to protect Plaintiffs' and Class Members' PHI and PII, and in intentionally misusing and/or disclosing their PHI and PII, Defendant acted with intentional malice and oppression and in conscious disregard of Plaintiffs' and Class Members' rights to have such information kept confidential and private. Plaintiffs, therefore, seeks an award of damages on behalf of themselves and the Class.

Sixth Count
Unjust Enrichment (In the Alternative)
(On Behalf of Plaintiffs and Class Members)

144. Plaintiffs re-allege paragraphs 1-84 as if fully set forth herein. Plaintiffs bring this claim individually and on behalf of all Class Members. This count is plead in the alternative to the breach of contract count above.

145. Upon information and belief, Defendant funds its data security measures entirely from its general revenue, including payments made by or on behalf of Plaintiffs and the Class Members.

146. As such, a portion of the payments made by or on behalf of Plaintiffs and the Class Members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendant.

147. Plaintiffs and Class Members conferred a monetary benefit on Defendant. Specifically, they purchased goods and services from Defendant and/or its agents and in so doing provided Defendant with their PHI and PII. In exchange, Plaintiffs and Class Members should have received from Defendant the goods and services that were the subject of the transaction and have their PHI and PII protected with adequate data security.

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

149. In particular, Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs and Class Members' Personal Information. Instead of providing a reasonable level of security that would have prevented the hacking incident, Defendant instead calculated to increase its own profits at the expense of

Plaintiffs and Class Members by utilizing cheaper, ineffective security measures. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite security.

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

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

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

153. If Plaintiffs and Class Members knew that Defendant had not reasonably secured their PHI, they would not have agreed to provide their PHI and PII to Defendant.

154. Plaintiffs and Class Members have no adequate remedy at law.

155. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (a) actual identity theft; (b) the loss of the opportunity of how their PHI and PII are used; (c) the compromise, publication, and/or theft of their PHI and PII; (d) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PHI and PII; (e) lost opportunity costs associated with efforts 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; (f) the continued risk to their PHI and PII, 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 PHI and PII in their continued possession; and (g) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PHI and PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

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

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

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs pray for judgment as follows:

a) For an Order certifying this action as a class action and appointing Plaintiffs and their counsel to represent the Class;

b) For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and Class Members' PHI and PII, and from refusing to issue prompt, complete and accurate disclosures to Plaintiffs and Class Members;

c) For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of PHI and PII compromised during the Data Breach;

d) For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

e) Ordering Defendant to pay for not less than ten years of credit monitoring services for Plaintiffs and the Class;

f) For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

g) For an award of punitive damages, as allowable by law;

h) For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

i) Pre- and post-judgment interest on any amounts awarded; and

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

JURY TRIAL DEMANDED

Plaintiffs demand a trial by jury on all claims so triable.

Dated: January 17, 2023

Respectfully Submitted,

/s/ John C. Whitfield, Esq.
John C. Whitfield (KY Bar #76410)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
19 North Main Street
Madisonville, KY 42431
T: (270) 821-0656
F: (270) 825-1163
Email: jwhitfield@milberg.com

MILBERG COLEMAN PHILLIPS GROSSMAN PLLC
Gary M. Klinger (*pro hac vice forthcoming)*
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
T: (865) 247-0047
gklinger@milberg.com

SHUB LAW FIRM LLC
Jonathan Shub (*pro hac vice forthcoming*)
Benjamin F. Johns
134 Kings Hwy E., Fl. 2,
Haddonfield, NJ 08033
T: (856) 772-7200
F: (856) 210-9088
jshub@shublawyers.com
bjohns@shublawyers.com

THE FINLEY FIRM, PC
MaryBeth V. Gibson (*pro hac* forthcoming)
Georgia Bar No. 725843
3535 Piedmont Road
Building 14, Suite 230
Atlanta, GA 30305
Telephone: (404) 978-6971
Fax: (404) 320- 9978
mgibson@thefinleyfirm.com

LOVE CONSUMER LAW
John A. Love
GA Bar. No 459155
2500 Northwinds Parkway
Suite 330
Alpharetta, GA 30009
(tel.) 404.855.3600
(fax) 404.301.2300
tlove@loveconsumerlaw.com

Attorneys for Plaintiffs and the Proposed Class

CERTIFICATE OF SERVICE

The undersigned hereby certifies that on January 17, 2023 the foregoing document was filed via the Court's ECF system, which will cause a true and correct copy of the same to be served electronically on all ECF-registered counsel of record.

/s/ John C. Whitfield
John C. Whitfield