# Exhibit A1

**UNITED STATES DISTRICT COURT**
**EASTERN DISTRICT OF KENTUCKY**
**LEXINGTON DIVISION**

| | |
|---|---|
| VIRGINIA HILEY, individually and on behalf of all others similarly situated,<br><br>Plaintiff,<br><br>v.<br><br>CORRECTCARE INTEGRATED HEALTH, LLC,<br><br>Defendant. | CASE NO:<br><br>**JURY DEMAND**<br><br>**CLASS ACTION** |

## CLASS ACTION COMPLAINT

Plaintiff Virginia Hiley ("Plaintiff"), individually and on behalf of all others similarly situated, brings this Class Action Complaint and alleges the following against Defendant CorrectCare Integrated Health, LLC ("CorrectCare" or "Defendant"), based upon personal knowledge with respect to Plaintiff 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 private health information ("PHI") of the Plaintiff and the putative Class Members. CorrectCare is a vendor that works with various customers in the prison industry "to facilitate access to appropriate medical providers and to manage the claims

payment process while minimizing costs within the correctional environment."[1] Over the course of this work, CorrectCare is entrusted with peoples' highly sensitive information.

2. According to CorrectCare, the PHI compromised in the Data Breach included names, dates of birth, Social Security Numbers and certain "limited health information, such as a diagnosis code and/or CPT code."[2]

3. Social Security numbers 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.

4. 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. 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, but it has only recently begun contacting Class Members.[3] "Further investigation" by the company revealed that patient information contained in these file directories may have been exposed as early as January 22, 2022.

5. 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.[4]

---

[1] *See* https://www.linkedin.com/company/correctcare-integrated-health/ (last visited December 5, 2022).
[2] *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).
[3] *Id.*
[4] "Important information on Data Breach." https://doc.louisiana.gov/data-breach-louisiana-doc/#:~:text=is%20potentially%20affected%3F-

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 almost 500,000 individuals had been exposed.[5]

6. Plaintiff brings this class action lawsuit on behalf of herself and all those similarly situated to address Defendant's inadequate safeguarding of Class Members' PHI that it collected and maintained, and for failing to provide timely and adequate notice to Plaintiff and other Class Members that their sensitive information was unsecured and left open to the unauthorized access of any unknown third party.

## PARTIES

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

8. Plaintiff's PHI was stored and handled by CorrectCare. Plaintiff Hiley was formerly incarcerated in Louisiana. During these time periods, she received medical treatment for, among other things, a broken finger, dental check-up, and wellness visits – the claims for which were, upon information and belief, processed by CorrectCare. On or around 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.

9. 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.

---

,The%20exposure%20of%20two%20file%20directories%20on%20a%20single%20server,%2C%20and%20July%207%2C%202022. (last accessed December 5, 2022).

[5] "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 December 5, 2022).

10. As a result of Defendant's conduct, Plaintiff suffered actual damages including, without limitation, time and expenses related to monitoring her 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. Plaintiff 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.

11. Defendant CorrectCare is a Kentucky entity with a principal place of business and headquarters in Fayette County, with an address at 1218 South Broadway, Suite 250, Lexington, Kentucky.

## JURISDICTION AND VENUE

12. This Court has subject matter jurisdiction over this controversy pursuant to 28 U.S.C. § 1332(d). 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.

13. This Court has personal jurisdiction over Defendant because it is authorized to and does conduct substantial business in this District, and is a citizen of this District by virtue of its headquarters and principal place of business being located in this District.

14. 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.

## COMMON FACTUAL ALLEGATIONS

15. Plaintiff and the proposed Class are individuals who had their PHI entrusted to CorrectCare. As noted above, CorrectCare is a medical claims processor servicing corrections facilities.[6]

16. Plaintiff brings 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 Plaintiff and other members of the class that such information had been compromised.

### CorrectCare's Unsecure Data Management and Disclosure of Data Breach

17. Plaintiff and Class Members provided their PHI 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.

18. Plaintiff and Class Member's PHI 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.

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

[6] "CorrectCare Integrated Health." https://www.corrections.direct/united-states/lexington/corrections/correctcare-integrated-health-3755 (last accessed December 5, 2022).

20. 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.

21. 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."[7]

22. After conducting an initial investigation, CorrectCare "determined patient information contained in these file directories may have been exposed as early as January 22, 2022."[8] CorrectCare noted that the patient information affect "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."[9]

23. 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 notify Plaintiff that her information was compromised.

**Plaintiff and the Class Have Suffered Injury as a Result of CorrectCare's Data Mismanagement**

24. As a result of Defendant's failure to implement and follow even the most basic security procedures, Plaintiff's and Class Members' PHI has been publicly exposed. Plaintiff 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.

[7] *See* n. 1.
[8] *Id.*
[9] *Id.*

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

26. Plaintiff 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.

27. 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.[10]

28. 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.[11]

29. 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.[12]

---

[10] *2022 Breach Barometer*, PROTENUS, https://www.protenus.com/breach-barometer-report (last accessed on Nov. 30, 2022).

[11] 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 November 30, 2022).

[12] *Cost of a Data Breach Report 2022*, IBM Security, https://www.ibm.com/downloads/cas/3R8N1DZJ (last visited November 30, 2022).

30. PII/PHI is a valuable property right.[13] The value of PII/PHI as a commodity is measurable.[14] "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."[15] American companies are estimated to have spent over $19 billion on acquiring personal data of consumers in 2018.[16] 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.

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

---

[13] *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...").

[14] *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 November 30, 2022).

[15] *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.

[16] *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/.

32. PHI is particularly valuable and has been referred to as a "treasure trove for criminals."[17] A cybercriminal who steals a person's PHI can end up with as many as "seven to 10 personal identifying characteristics of an individual."[18] 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.[19]

33. Personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[20] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[21] 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.[22] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[23] According to a report released by the Federal

---

[17] *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 November 30, 2022).

[18] *Id.*

[19] 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 November 30, 2022).

[20] 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 November 30, 2022).

[21] 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 November 30, 2022).

[22] 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 November 30, 2022).

[23] *In the Dark*, VPNOverview.com, 2019, https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed on Nov. 30, 2022).

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.[24]

34. Criminals can use stolen PII/PHI to extort a financial payment by "leveraging details specific to a disease or terminal illness."[25] 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."[26]

35. 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."[27]

36. 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.

37. Indeed, 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

---

[24] *See Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain*, FBI CYBER DIVISION (Apr. 8, 2014), https://www.illuminweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systems-cyber-intrusions.pdf.
[25] *See* n.16, *supra*.
[26] *Id.*
[27] 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.

is compromised, 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."[28]

38. 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.[29]

39. In fact, according to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in the past year.[30]

40. 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)."[31]

---

[28] 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).

[29] 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).

[30] *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).

[31] 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-

41. 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.[32]

42. 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 Plaintiff and Class Members.

43. Plaintiff 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.

44. Once PHI is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or contained against future misuse. For this reason, Plaintiff and Class members will need to maintain these heightened measures for years, and possibly their

---

firms-they-are-targeted-by-hackers-idUSKBN0GK24U20140820 (last visited November 30, 2022).

[32] 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).

entire lives, as a result of CorrectCare' conduct. Further, the value of Plaintiff's and Class members' PHI has been diminished by its exposure in the Data Breach.

45. As a result of CorrectCare's data security failures, Plaintiff and Class members are at substantial risk of suffering identity theft and fraud or misuse of their PHI.

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

47. For the reasons mentioned above, CorrectCare's conduct, which allowed the Data Breach to occur, caused Plaintiff and members of the Class these significant injuries and harm.

48. Plaintiff brings this class action against CorrectCare for its failure to properly secure and safeguard PHI and for failing to provide timely, accurate, and adequate notice to Plaintiff and other class members that their PHI had been compromised.

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

## CLASS ACTION ALLEGATIONS

50. Plaintiff brings this action on behalf of herself and on behalf of all other persons similarly situated.

51. Plaintiff proposes the following Class definition, subject to amendment as appropriate:

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

52. 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.

53. Plaintiff reserves 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).

54. 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.

55. 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 Plaintiff(s)' and Class Members' PHI;

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;

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

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

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

i. Whether Plaintiff(s) 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 Plaintiff(s) and Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

56. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's PHI, like that of every other Class member, was compromised in the Data Breach.

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

58. Predominance. Defendant has engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff's 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.

59. 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.

60. 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.

61. 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 Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their PHI;

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

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

62. 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 Plaintiff and Class Members)

63. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

64. CorrectCare (by and through its customers) required Plaintiff and Class Members to submit non-public personal information in order to obtain healthcare/medical services.

65. 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 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.

66. Defendant owed a duty of care to Plaintiff 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.

67. 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.

68. 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.

69. 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.

70. 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.

71. Defendant breached its duties, and thus were negligent, by failing to use reasonable measures to protect Class Members' PHI. 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;

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;

e. Failing to detect in a timely manner that Class Members' PHI 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

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

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

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

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

76. Plaintiff 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 Plaintiff and Class Members)**

77. Plaintiff re-allege the above allegations as if fully set forth herein.

78. When Plaintiff and Class Members provided their PHI 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.

79. Defendant CorrectCare solicited, offered, and invited Class Members to provide their PHI as part of Defendant's regular business practices. Plaintiff(s) and Class Members accepted Defendant's offers and provided their PHI to Defendant.

80. In entering into such implied contracts, Plaintiff 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.

81. Plaintiff and Class Members paid money to Defendant 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.

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

83. Plaintiff and Class Members would not have entrusted their PHI 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.

84. Plaintiff and Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

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

86. 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.

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

88. Plaintiff 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 Plaintiff(s) and All Class Members)**

89. Plaintiff re-alleges the above allegations as if fully set forth herein.

90. 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 Plaintiff' and Class Members' PHI.

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

92. 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.

93. Defendant breached its duties to Plaintiff 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 Plaintiff(s)' and Class Members' PHI.

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

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

96. The injury and harm suffered by Plaintiff 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 Plaintiff and Class Members to experience the foreseeable harms associated with the exposure of their PHI.

97. As a direct and proximate result of Defendant's negligent conduct, Plaintiff 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 Plaintiff and Class Members)**

98. Plaintiff re-alleges the above allegations as if fully set forth herein.

99. In light of the confidential medical relationship between Defendant CorrectCare and Plaintiff(s) and Class Members, whereby Defendant became guardian of Plaintiff(s)' and Class Members' PHI, Defendant became a fiduciary by its undertaking and guardianship of the PHI, to act primarily for Plaintiff(s) and Class Members, (1) for the safeguarding of Plaintiff(s)' and Class Members' PHI; (2) to timely notify Plaintiff(s) 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.

100. Defendant has a fiduciary duty to act for the benefit of Plaintiff(s) 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.

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

102. Defendant breached its fiduciary duties to Plaintiff(s) and Class Members by failing to encrypt and otherwise protect the integrity of the systems containing Plaintiff(s)' and Class Members' PHI.

103. Defendant breached its fiduciary duties owed to Plaintiff(s) and Class Members by failing to timely notify and/or warn Plaintiff(s) and Class Members of the Data Breach.

104. Defendant breached its fiduciary duties to Plaintiff(s) and Class Members by otherwise failing to safeguard Plaintiff(s)' and Class Members' PHI.

105. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff(s) 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; (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, 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 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 Plaintiff(s) and Class Members; and (vii) the diminished value of Defendant's services they received.

106. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiff(s) 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 Plaintiff and All Class Members)**

107. Plaintiff re-allege the above allegations as if fully set forth herein.

108. Plaintiff(s) and Class Members had a reasonable expectation of privacy in the PHI Defendant mishandled.

109. Defendant's conduct as alleged above intruded upon Plaintiff(s)' and Class Members' seclusion under common law.

110. By intentionally failing to keep Plaintiff(s)' and Class Members' PHI safe, and by intentionally misusing and/or disclosing said information to unauthorized parties for unauthorized use, Defendant intentionally invaded Plaintiff(s)' and Class Members' privacy by:

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

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

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

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

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

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

114. The conduct described above was at or directed at Plaintiff and the Class Members.

115. As a proximate result of such intentional misuse and disclosures, Plaintiff's and Class Members' reasonable expectations of privacy in their PHI was unduly frustrated and thwarted. Defendant's conduct amounted to a substantial and serious invasion of Plaintiff's 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.

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

**Sixth Count**
**Unjust Enrichment**
**(On Behalf of Plaintiff and Class Members)**

117. Plaintiff re-alleges the above allegations as if fully set forth herein. Plaintiff brings this claim individually and on behalf of all Class Members. This count is plead in the alternative to the breach of contract count above.

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

119. As such, a portion of the payments made by or on behalf of Plaintiff 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.

120. Plaintiff 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. In exchange, Plaintiff and Class Members should have received from Defendant the goods and services that were the subject of the transaction and have their PHI protected with adequate data security.

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

122. In particular, Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's 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 Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff 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.

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

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

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

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

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

128. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (a) actual identity theft; (b) the loss of the opportunity of how their PHI is used; (c) the compromise, publication, and/or theft of their PHI; (d) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PHI; (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, 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 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 compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

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

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

## PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment as follows:

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

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

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

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

e) Ordering CorrectCare to pay for not less than ten years of credit monitoring services for Plaintiff 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**

Plaintiff demands a trial by jury on all claims so triable.

Dated: December 7, 2022

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

**SHUB LAW FIRM LLC**
Jonathan Shub*
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

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

*Attorneys for Plaintiff and the Proposed Class*

AO 440 (Rev. 06/12) Summons in a Civil Action

# UNITED STATES DISTRICT COURT

for the

Eastern District of Kentucky

Virginia Hiley, individually and on behalf of all others similarly situated

*Plaintiff(s)*

v.

CorrectCare Integrated Health, LLC

*Defendant(s)*

Civil Action No.

## SUMMONS IN A CIVIL ACTION

To: *(Defendant's name and address)*

CorrectCare Integrated Health, LLC
c/o Registered Agent, Anthony Q. Baxter
1218 South Broadway, Suite 250
Lexington, KY 40504

A lawsuit has been filed against you.

Within 21 days after service of this summons on you (not counting the day you received it) — or 60 days if you are the United States or a United States agency, or an officer or employee of the United States described in Fed. R. Civ. P. 12 (a)(2) or (3) — you must serve on the plaintiff an answer to the attached complaint or a motion under Rule 12 of the Federal Rules of Civil Procedure. The answer or motion must be served on the plaintiff or plaintiff's attorney, whose name and address are: John C. Whitfield, Esq., Milberg Coleman Bryson Phillips Grossman, PLLC, 19 North Main St., Madisonville, KY 42431

If you fail to respond, judgment by default will be entered against you for the relief demanded in the complaint. You also must file your answer or motion with the court.

*CLERK OF COURT*

Date: _____

_____
*Signature of Clerk or Deputy Clerk*

Civil Action No.

**PROOF OF SERVICE**

***(This section should not be filed with the court unless required by Fed. R. Civ. P. 4 (l))***

This summons for *(name of individual and title, if any)* _____ was received by me on *(date)* _____ .

❒ I personally served the summons on the individual at *(place)* _____ on *(date)* _____ ; or

❒ I left the summons at the individual's residence or usual place of abode with *(name)* _____ , a person of suitable age and discretion who resides there, on *(date)* _____ , and mailed a copy to the individual's last known address; or

❒ I served the summons on *(name of individual)* _____ , who is designated by law to accept service of process on behalf of *(name of organization)* _____ on *(date)* _____ ; or

❒ I returned the summons unexecuted because _____ ; or

❒ Other *(specify):*

My fees are $ _____ for travel and $ _____ for services, for a total of $ 0.00 .

I declare under penalty of perjury that this information is true.

Date: _____

_____
*Server's signature*

_____
*Printed name and title*

_____
*Server's address*

Additional information regarding attempted service, etc:

JS 44 (Rev. 04/21)

# CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. *(SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)*

## I. (a) PLAINTIFFS

Virginia Hiley, individually and on behalf of all others similarily situated

**(b)** County of Residence of First Listed Plaintiff _____
*(EXCEPT IN U.S. PLAINTIFF CASES)*

**(c)** Attorneys *(Firm Name, Address, and Telephone Number)*
John C. Whitfield, Esq., Milberg Coleman Bryson Phillips Grossman, PLLC, 19 N. Main St., Madisonville, KY 42431; T: 270-821-0656

## DEFENDANTS

CorrectCare Integrated Health, LLC

County of Residence of First Listed Defendant _____
*(IN U.S. PLAINTIFF CASES ONLY)*

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys *(If Known)*

## II. BASIS OF JURISDICTION *(Place an "X" in One Box Only)*

- ☐ 1 U.S. Government Plaintiff
- ☐ 3 Federal Question *(U.S. Government Not a Party)*
- ☐ 2 U.S. Government Defendant
- ☒ 4 Diversity *(Indicate Citizenship of Parties in Item III)*

## III. CITIZENSHIP OF PRINCIPAL PARTIES *(Place an "X" in One Box for Plaintiff and One Box for Defendant)*
*(For Diversity Cases Only)*

| | PTF | DEF | | PTF | DEF |
|---|---|---|---|---|---|
| Citizen of This State | ☐ 1 | ☐ 1 | Incorporated *or* Principal Place of Business In This State | ☐ 4 | ☒ 4 |
| Citizen of Another State | ☒ 2 | ☐ 2 | Incorporated *and* Principal Place of Business In Another State | ☐ 5 | ☐ 5 |
| Citizen or Subject of a Foreign Country | ☐ 3 | ☐ 3 | Foreign Nation | ☐ 6 | ☐ 6 |

## IV. NATURE OF SUIT *(Place an "X" in One Box Only)*

Click here for: Nature of Suit Code Descriptions.

**CONTRACT**
- ☐ 110 Insurance
- ☐ 120 Marine
- ☐ 130 Miller Act
- ☐ 140 Negotiable Instrument
- ☐ 150 Recovery of Overpayment & Enforcement of Judgment
- ☐ 151 Medicare Act
- ☐ 152 Recovery of Defaulted Student Loans (Excludes Veterans)
- ☐ 153 Recovery of Overpayment of Veteran's Benefits
- ☐ 160 Stockholders' Suits
- ☐ 190 Other Contract
- ☐ 195 Contract Product Liability
- ☐ 196 Franchise

**TORTS**

PERSONAL INJURY
- ☐ 310 Airplane
- ☐ 315 Airplane Product Liability
- ☐ 320 Assault, Libel & Slander
- ☐ 330 Federal Employers' Liability
- ☐ 340 Marine
- ☐ 345 Marine Product Liability
- ☐ 350 Motor Vehicle
- ☐ 355 Motor Vehicle Product Liability
- ☒ 360 Other Personal Injury
- ☐ 362 Personal Injury - Medical Malpractice

PERSONAL INJURY
- ☐ 365 Personal Injury - Product Liability
- ☐ 367 Health Care/ Pharmaceutical Personal Injury Product Liability
- ☐ 368 Asbestos Personal Injury Product Liability

PERSONAL PROPERTY
- ☐ 370 Other Fraud
- ☐ 371 Truth in Lending
- ☐ 380 Other Personal Property Damage
- ☐ 385 Property Damage Product Liability

**FORFEITURE/PENALTY**
- ☐ 625 Drug Related Seizure of Property 21 USC 881
- ☐ 690 Other

**LABOR**
- ☐ 710 Fair Labor Standards Act
- ☐ 720 Labor/Management Relations
- ☐ 740 Railway Labor Act
- ☐ 751 Family and Medical Leave Act
- ☐ 790 Other Labor Litigation
- ☐ 791 Employee Retirement Income Security Act

**IMMIGRATION**
- ☐ 462 Naturalization Application
- ☐ 465 Other Immigration Actions

**BANKRUPTCY**
- ☐ 422 Appeal 28 USC 158
- ☐ 423 Withdrawal 28 USC 157

**INTELLECTUAL PROPERTY RIGHTS**
- ☐ 820 Copyrights
- ☐ 830 Patent
- ☐ 835 Patent - Abbreviated New Drug Application
- ☐ 840 Trademark
- ☐ 880 Defend Trade Secrets Act of 2016

**SOCIAL SECURITY**
- ☐ 861 HIA (1395ff)
- ☐ 862 Black Lung (923)
- ☐ 863 DIWC/DIWW (405(g))
- ☐ 864 SSID Title XVI
- ☐ 865 RSI (405(g))

**FEDERAL TAX SUITS**
- ☐ 870 Taxes (U.S. Plaintiff or Defendant)
- ☐ 871 IRS—Third Party 26 USC 7609

**OTHER STATUTES**
- ☐ 375 False Claims Act
- ☐ 376 Qui Tam (31 USC 3729(a))
- ☐ 400 State Reapportionment
- ☐ 410 Antitrust
- ☐ 430 Banks and Banking
- ☐ 450 Commerce
- ☐ 460 Deportation
- ☐ 470 Racketeer Influenced and Corrupt Organizations
- ☐ 480 Consumer Credit (15 USC 1681 or 1692)
- ☐ 485 Telephone Consumer Protection Act
- ☐ 490 Cable/Sat TV
- ☐ 850 Securities/Commodities/ Exchange
- ☐ 890 Other Statutory Actions
- ☐ 891 Agricultural Acts
- ☐ 893 Environmental Matters
- ☐ 895 Freedom of Information Act
- ☐ 896 Arbitration
- ☐ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
- ☐ 950 Constitutionality of State Statutes

**REAL PROPERTY**
- ☐ 210 Land Condemnation
- ☐ 220 Foreclosure
- ☐ 230 Rent Lease & Ejectment
- ☐ 240 Torts to Land
- ☐ 245 Tort Product Liability
- ☐ 290 All Other Real Property

**CIVIL RIGHTS**
- ☐ 440 Other Civil Rights
- ☐ 441 Voting
- ☐ 442 Employment
- ☐ 443 Housing/ Accommodations
- ☐ 445 Amer. w/Disabilities - Employment
- ☐ 446 Amer. w/Disabilities - Other
- ☐ 448 Education

**PRISONER PETITIONS**

**Habeas Corpus:**
- ☐ 463 Alien Detainee
- ☐ 510 Motions to Vacate Sentence
- ☐ 530 General
- ☐ 535 Death Penalty

**Other:**
- ☐ 540 Mandamus & Other
- ☐ 550 Civil Rights
- ☐ 555 Prison Condition
- ☐ 560 Civil Detainee - Conditions of Confinement

## V. ORIGIN *(Place an "X" in One Box Only)*

☒ 1 Original Proceeding ☐ 2 Removed from State Court ☐ 3 Remanded from Appellate Court ☐ 4 Reinstated or Reopened ☐ 5 Transferred from Another District *(specify)* ☐ 6 Multidistrict Litigation - Transfer ☐ 8 Multidistrict Litigation - Direct File

## VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing ***(Do not cite jurisdictional statutes unless diversity)***:
28 U.S.C. 1332(d)

Brief description of cause:
Class Action data breach

## VII. REQUESTED IN COMPLAINT:

☒ CHECK IF THIS IS A **CLASS ACTION** UNDER RULE 23, F.R.Cv.P.

**DEMAND $** 5,000,000

CHECK YES only if demanded in complaint:
**JURY DEMAND:** ☒ Yes ☐ No

## VIII. RELATED CASE(S) IF ANY

*(See instructions):* JUDGE _____ DOCKET NUMBER _____

DATE
Dec 7, 2022

SIGNATURE OF ATTORNEY OF RECORD
/s/ John C. Whitfield, Esq.

**FOR OFFICE USE ONLY**

RECEIPT # _____ AMOUNT _____ APPLYING IFP _____ JUDGE _____ MAG. JUDGE _____