UNITED STATES DISTRICT COURT

WESTERN DISTRICT OF KENTUCKY

CHRISTIAN SMITH. on behalf of himself and all others similarly situated, **Plaintiff,** **v.** **KENTUCKY COUNSELING CENTER, LLC,** **Defendant.**	**CASE NO.:** **CLASS ACTION** **COMPLAINT FOR DAMAGES, EQUITABLE, DECLARATORY AND INJUNCTIVE RELIEF** **DEMAND FOR JURY TRIAL**

Plaintiff, Christian Smith ("Plaintiff"), individually, by and through his undersigned counsel, brings this class action lawsuit against Kentucky Counseling Center, LLC ("KCC"), on behalf of himself and all others similarly situated, and alleges, based upon information and belief and the investigation of his counsel as follows:

INTRODUCTION

1. This is a putative class action lawsuit brought by current and former patients of KCC against Defendant for its failure to properly secure and safeguard the personally identifiable information of its patients, and for its failure to provide timely, accurate and adequate notice that such information had been compromised.

2. On January 4, 2019, KCC discovered that nearly one month earlier, one of its employees obtained and exfiltrated a document containing the personal health information ("PHI") and other personally identifiable information (collectively "PII") of approximately 16,440 KCC patients ("Data Brach"). The employee used an anonymous Internet file sharing service to subsequently disseminate the PII to unauthorized individuals.[1] The exposed PII included names, addresses, dates of birth, emails, phone numbers, Social Security Numbers, sex, marital and employment status, insurance payer and insurance numbers.

---

[1] Personally identifiable information generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual. PII also is generally defined to include certain identifiers that do not on their face name an individual, but are considered to be particularly sensitive and/or valuable if in the wrong hands (for example, Social Security number, passport number, driver's license number, financial account number). Under the Health Insurance Portability and Accountability Act, 42 U.S.C. § 1320d *et seq.* ("HIPAA"), protected health information ("PHI") is considered to be individually identifiable information relating to the past, present, or future health status of an individual that is created, collected, or transmitted, or maintained by a HIPAA-covered entity in relation to the provision of healthcare, payment for healthcare services, or use in healthcare operations. 45 C.F.R. § 160.103. Health information such as diagnoses, treatment information, medical test results, and prescription information are considered protected health information under HIPAA, as are national identification numbers and demographic information such as birth dates, gender, ethnicity, and contact and emergency contact information. https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html.

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

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

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

6. Plaintiff, on behalf of all others similarly situated, alleges claims for negligence, negligence per se, invasion of privacy, breach of implied contract, unjust enrichment, breach of fiduciary duty, breach of confidence and violation of the Kentucky Consumer Protection Act and seeks to compel Defendant to fully and accurately disclose the nature of the information that has been compromised and to adopt reasonably sufficient security practices to safeguard patient PII that remains in its custody in order to prevent incidents like the Data Breach from reoccurring in the future.

PARTIES

7. Plaintiff, Christian Smith, is a resident of Louisville, Kentucky and a former patient of KCC. On or about February 8, 2019, Mr. Smith received notice from KCC that his PII, along with more than 16,000 other patients, had been exfiltrated from KCC's computers and disseminated to unauthorized third parties.

8. After being notified of the Data Breach, Mr. Smith contacted Trans Union and Equifax to obtain copies of his credit report. He subsequently placed freezes on his credit with those two credit bureaus and signed up for credit monitoring services in an effort to mitigate the effects of the Data Breach.

9. Since the announcement of the Data Breach, Mr. Smith continues to monitor his accounts in an effort to detect and prevent any misuses of his personal information.

10. Mr. Smith has, and continues to, spend his valuable time to protect the integrity of his medical records, finances and credit – time which he would not have had to expend but for the Data Breach.

11. Plaintiff suffered actual injury from having his PII stolen as a result of the Data Breach including, but not limited to: (a) paying monies to KCC for its goods and services which he would not have had if KCC disclosed that it lacked computer systems and data security practices adequate to safeguard consumers' PII from theft; (b) damages to and diminution in the value of his PII—a form of intangible property that the Plaintiff entrusted to KCC as a condition for health services; (c) loss of his privacy; .(d) imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII being exposed to criminals.

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

13. Defendant Kentucky Counseling Center is a Kentucky limited liability company headquartered at 4835 Poplar Level Rd., #110, Louisville, Kentucky. KCC provides counseling, psychiatry, and targeted case management services for children and adults in 10 locations throughout Kentucky.

JURISDICTION AND VENUE

14. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. There are approximately 30,000 putative class members, and at least some members of the proposed Class have a different citizenship from KCC.

15. This Court has jurisdiction over the Defendant as it operates in this District, and the data implicated in this Breach was generated and maintained in this District. KCC is also headquartered in this District.

16. Plaintiff was a KCC patient that received health services in this District where his PII was also maintained, and where the breach occurred which led to him sustaining damage. Through its business operations in this District. KCC intentionally avails itself of the markets within this District to render the exercise of jurisdiction by this Court just and proper.

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

STATEMENT OF FACTS

A. The KCC Data Breach

18. On January 4, 2019, KCC learned that one of its employees improperly obtained and exfiltrated data containing the sensitive PII of 16,440 of its current and former patients. The KCC employee uploaded the data to an anonymous file sharing service, and subsequently sent a hyperlink of the list to a former KCC employee.

19. As a result of the purposeful action of one of its employees, the sensitive patient PII was publicly exposed for nearly a month, for anyone, including a host of malicious actors to review, download and use. The exposed PII includes the most sensitive types of personal information including, but not limited to, patient names, dates of birth, health insurance information and/or information about medical care received at KCC and Social Security numbers.

20. On February 8, 2019, KCC sent a letter to affected patients stating, in relevant part, the following:

> I am writing to make you aware of a recent incident at Kentucky Counseling Center (KCC). On January 4, 2019, a former KCC staff member reported receiving an

> email containing a link to a KCC patient list. KCC then began an investigation into the former staff member's report. Based on our investigation to date, we believe a KCC staff member took the list without authorization from our computer system on December 6, 2018. We believe that same individual used an anonymous Internet file sharing service to email the list to the former KCC staff member. The individual we believe to be responsible for the email is no longer working with KCC.
>
> You are receiving this letter because you were included on the patient list mentioned above, While we do not believe the individual took the patient list to cause harm to individuals on the list, we wanted to make you aware of these circumstances out of an abundance of caution.
>
> The type of information on the list varied for different people but may have included the following: name; address; date of birth; email; phone number; Social Security Number; sex; marital and employment status; insurance payer and insurance number. The list did not include any clinical information other than the date of the last and/or next appointment for some individuals; and, in some cases, the names of KCC clinicians involved in an individual's care.
>
> We have taken a number of steps to prevent this type of event from happening in the future, including strengthening our password requirements and training KCC staff members to provide a separate form of authentication, in addition to a username and password, to access our computer system.
>
> We recommend you remain vigilant to the possibility of fraud and identity theft by reviewing account statements and monitoring free credit reports for unauthorized activity. To assist you, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (myTrueIdentity) for one year provided by TransUnion Interactive….[2]

B. Prevalence of Cyber Attacks and the Particular Susceptibility of Healthcare Systems

21. Over the past several years, data breaches have become pervasive. In 2016, the number of U.S. data breaches surpassed 1,000, representing a record high and a forty percent increase from the previous year.[3] In 2017 a record high 1,579 breaches were reported, representing

---

[2] See, letter from KCC to Christian Smith, February 8, 2019, attached hereto as Exhibit A.

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

a 44.7% increase over 2016.[4] In 2018, the healthcare sector suffered the second largest number of breaches among all major sectors and had the highest rate of exposure per breach.[5]

22. Hospital data breaches in particular have continued to rapidly increase. According to the 2019 HIMSS Cybersecurity Survey, 82 percent of participating hospitals reported having a significant security incident within the last 12 months, with a majority of those being caused by "bad actors…"[6]

23. As pointed out in Verizon's 2017 Protected Health Information Data Breach Report ("DBR"), the healthcare industry is "the only industry in which internal actors are the biggest threat to an organization."[7] The DBR found that of the 1,368 data breaches it examined, "58% of the incidents involved insiders."[8]

24. "Hospitals have emerged as a primary target because they sit on a gold mine of sensitive personally identifiable information for thousands of patients at any given time. From social security and insurance policies to next of kin and credit cards, no other organization, including credit bureaus, have so much monetizable information stored in their data centers."[9]

25. Indeed, healthcare related data is among the most sensitive, and personally consequential when compromised. A report focusing on health-care breaches found that the "average

---

[4] *2017 Annual Data Breach Year-End Review*, Identity Theft Resource Center ("ITRC"), https://www.idtheftcenter.org/2017-data-breaches/.

[5] *2018 End -of-Year Data Breach Report*, ITRC, 2018, https://www.idtheftcenter.org/2018-data-breaches/.

[6] https://www.himss.org/2019-himss-cybersecurity-survey.

[7] *Protected Health Information Data Breach Report*, Verizon (2018), https://enterprise.verizon.com/resources/reports/2018/protected_health_information_data_breach_report.pdf

[8] *Id.*

[9] *How to Safeguard Hospital Data from Email Spoofing Attacks*, Inside Digital Health, April 4, 2019, https://www.idigitalhealth.com/news/how-to-safeguard-hospital-data-from-email-spoofing-attacks.

total cost to resolve an identity theft-related incident…came to about $20,000," and that the victims were routinely forced to pay out-of-pocket costs for health care they did not receive in order to restore coverage. [10] Almost 50 percent of the victims lost their health care coverage as a result of the incident, while nearly one-third said their insurance premiums went up after the event. Forty percent of the customers were never able to resolve their identity theft at all.[11]

26. "Unfortunately, by the time medical identity theft is discovered, the damage has been done. Forty percent of consumers say that they found out they were a victim of medical identity theft only when they received collection letters from creditors for expenses that thieves incurred in their name. As a result, the consequences of medical identity theft are frequently severe, stressful and expensive to resolve." [12]

27. These consequences are further exacerbated when the compromised PII includes Social Security numbers, which make it possible for thieves to perpetrate the most serious types of fraud such as filing tax returns, seeking unemployment benefits, or even applying for a job using a false identity. Each of these fraudulent activities is difficult to detect and may not be uncovered until the number has already been used in a fraudulent transaction. Moreover, it is no easy task to cancel a stolen Social Security number, and even then "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[13]

---

[10] Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET, March 3, 2010, https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/.

[11] *Id.*

[12] *The Potential Damages and Consequences of Medical Identity Theft and Healthcare Data Breaches*, Experian (April 2010), https://www.experian.com/assets/data-breach/white-papers/consequences-medical-id-theft-healthcare.pdf.

[13] Naylor, B., *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR, Feb. 9, 2015, http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft.

28. As a long-standing member of the healthcare community, KCC knew the importance of safeguarding patient PII entrusted to it and of the foreseeable consequences of a breach. Despite this knowledge, however, KCC failed to take adequate cyber-security measures to prevent the most basic and common type of breach from happening.

C. Defendant Acquires, Collects, and Stores Plaintiff's and Class Members' PII

29. As a condition for obtaining health services, KCC requires that its patients provide them with highly sensitive personal information.

30. Defendant subsequently acquired, collected, and stored a massive amount of protected health related information and other personally identifiable information on its patients.

31. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PII, KCC assumed legal and equitable duties to those individuals and knew or should have known that it was responsible for protecting such PII from disclosure.

32. Plaintiff and the Class Members have taken reasonable steps to maintain the confidentiality of their PII. Plaintiff and the Class Members, as current and former patients, relied on KCC to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

33. Indeed, KCC maintains, as it must, a policy which specifically acknowledges its legal obligation to maintain the privacy of patient PII entrusted to it and to only disclose such information under limited circumstances, none of which are relevant here. Among other things, KCC affirmed its commitment to "maintaining client confidentiality in accordance with federal and state laws and ethics of the counseling profession."[14]

D. Defendant's Conduct Violates HIPAA and Industry Standard Practices

34. The Health Insurance Portability and Accountability Act ("HIPAA") enacts security provisions and data privacy responsibilities designed to keep patients' medical information safe.

---

[14] https://kentuckycounselingcenter.com/notice-of-privacy-policies/

HIPAA compliance provisions, commonly known as the Administrative Simplification Rules establish national standards for electronic transactions and code sets to maintain the privacy and security of protected health information.[15]

35. HIPAA provides specific privacy rules that require comprehensive administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of PHI is being properly maintained.[16]

36. Defendant's Breach resulted from a combination of deficiencies that show KCC failed to comply with safeguards mandated by HIPAA regulations and industry standards. KCC's security failures include, but are not limited to:

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

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

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

---

[15] HIPAA lists 18 type of information that qualify as PHI according to guidance from the Department of Health and Human Services Office for Civil Rights and includes: names, addresses, any dates including dates of birth, social security numbers and medical record numbers among others.

[16] 45 C.F.R. § 164.306 (Security standards and General rules); 45 C.F.R. § 164.308 (Administrative safeguards); 45 C.F.R. § 164.310 (Physical safeguards); 45 C.F.R. § 164.312 (Technical safeguards).

d. Failing to ensure compliance with HIPAA security standard rules by their workforce in violation of 45 C.F.R. § 164.306(a)(4);

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

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

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

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

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

E. Defendant Fails to Comply with FTC Guidelines

37. According to the Federal Trade Commission, the need for data security should be factored into all business decision-making.[17] To that end, the FTC has issued numerous guidelines identifying best data security practices that business should employ to protect against the unlawful exposure of PII.

[17] *Start With Security*, FTC, https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

38. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[18] The guidelines explain that businesses should: protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems. The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

39. The FTC recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[19]

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

41. KCC's failure to employ reasonable and appropriate measures to protect against unauthorized access to patient PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

---

[18] *Protecting Personal Information: A Guide for Business*, FTC, https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

[19] S*upra* at note 17.

42. KCC was at all times fully aware of its obligation to protect the PII of its patients because of its position as a trusted healthcare provider. KCC was also aware of the significant repercussions to its patients resulting from its failure to protect their PII.

F. Defendant Fails to Comply with Industry Standards

43. The healthcare industry continues to be a high value target among cybercriminals. In 2017, the U.S. healthcare sector experienced over 330 data breaches, a number which continued to grow in 2018 (363 breaches).[20] The costs of healthcare data breaches are among the highest across all industries, topping $380 per stolen record in 2017 as compared to the global average of $141 per record. *Id.* As a result, both the government and private sector have developed industry best standards to address this growing problem.

44. The Department of Health and Human Services' Office for Civil Rights ("DHHS") notes that, "[w]hile all organizations need to implement policies, procedures, and technical solutions to make it harder for hackers to gain access to their systems and data, this is especially important in the healthcare industry. Hackers are actively targeting healthcare organizations as they store large quantities of highly sensitive and valuable data." [21] DHHS highlights "several basic cybersecurity safeguards that can be implemented to improve cyber resilience which only require a relatively small financial investment, yet they can have a major impact on an organization's cybersecurity posture." *Id.* Most notably, organizations must properly encrypt PII in order to mitigate against misuse.

---

[20] *2018 End of Year Data Brach Report,* ITRC, 2018, https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_2018-End-of-Year-Aftermath_FINAL_V2_combinedWEB.pdf; https://www.ntiva.com/blog/10-cybersecurity-best-practices-for-the-healthcare-industry

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

45. The private sector has similarly identified the healthcare sector as being particularly vulnerable to cyber-attacks both because of the of value of the PII that it maintains and because, as an industry, it has been slow to adapt and respond to cybersecurity threats.[22]

46. Despite the abundance and availability of information regarding cybersecurity best practices for the healthcare industry, KCC chose to ignore them, a fact highlighted in its notification to affected patients in which it revealed that only after the Breach KCC is taking "a number of steps to prevent this type of event from happening in the future, including strengthening our password requirements and requiring KCC staff members to provide a separate form of authentication, in addition to a username and password, to access our computer system."[23]

47. KCC further represented that subsequent to the Data Breach it would now "implement additional technical safeguards…. [p]rovid[e] additional staff training on identifying unauthorized access,… and secur[e] a specialized cybersecurity firm to further assist us in implementing system-wide policies and procedures to help prevent a similar incident from occurring in the future."[24] Each of these preventative measures have long been cornerstones in the list of industry best practices. They were known, or should have been known by KCC, whose failure to heed and properly implement these practices directly led to the Data Breach and the unlawful exposure of its patients' PII.

G. Plaintiff and Class Members Suffered Damages

48. The ramifications of Defendant's failure to keep its Patients' PII secure are long lasting and severe. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

---

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

[23] Exhibit A, *supra* n.2.

[24] https://www.KCCcenter.com/KCC-counseling-center-notifies-individuals-of-possible-data-security-incident/

49. Victims of medical identity theft can suffer significant financial consequences. "In some cases, they paid the healthcare provider, repaid the insurer for services obtained by the thief, or they engaged an identity service provider or legal counsel to help resolve the incident and prevent future fraud."[25]

50. Moreover, resolution of medical identity theft is time consuming to resolve. "Due to HIPAA privacy regulations, victims of medical identity theft must be involved in the resolution of the crime. In many cases, victims struggle to reach resolution following a medical identity theft incident." *Id.* Consequently, they remain at "risk for further theft or errors in [their] healthcare records that could jeopardize medical treatments and diagnosis." *Id.*

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

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

53. Defendant had the resources necessary to prevent the Breach, but neglected to adequately invest in data security measures, despite their obligations to protect patient PII.

54. Had Defendant remedied the deficiencies in its systems and protocols and adopted security measures commonly used in the industry, it could have prevented the theft of PII.

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

[25] *Fifth Annual Study on Medical Identity Theft*, Ponemon Institute LLC, (February 2015), available at https://static.nationwide.com/static/2014_Medical_ID_Theft_Study.pdf?r=65.

harm from identity theft and fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and family in an effort to mitigate the actual and potential impact of the Data Breach on their lives.

56. The U.S. Department of Justice's Bureau of Justice Statistics found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems" and that "resolving the problems caused by identity theft [could] take more than a year for some victims."[26]

57. To date, KCC has offered patients only a 1-year membership in credit monitoring and identity protection services.[27] This offer is insufficient for several reasons. First, as discussed herein, victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft. One year is simply insufficient to mitigate the harms caused by this Breach. Second, the offer neither addresses, nor provides any compensation for the unauthorized release and disclosure of Plaintiff's and Class Members' PII. Finally, the offer places the burden on Plaintiff and Class Members, rather than on the Defendant, to investigate and protect themselves from Defendant's tortious acts. Rather than automatically enrolling Plaintiff and Class Members in credit monitoring services upon discovery of the breach, Defendant merely sent instructions "offering" the services to affected patients recommending they sign up for the services.

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

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

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

---

[26] *Victims of Identity Theft, 2012*, U.S. Department of Justice, Office of Justice Programs Bureau of Justice Statistics, December 2013, https://www.bjs.gov/content/pub/pdf/vit12.pdf.

[27] See, Exhibit A. ("To assist you, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (myTrueIdentity) for one year….")

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

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

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

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

CLASS ACTION ALLEGATIONS

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

> All persons in the United States whose PII was compromised as a result of the Data Breach announced by KCC in February 2019 (the "Class").

61. Plaintiff also seeks certification of a Kentucky-wide subclass defined as follows:

> All persons in the state of Kentucky whose PII was compromised as a result of the Data Breach announced by KCC in February 2019 (the "Class").

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

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

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

65. **Numerosity. Fed. R. Civ. P. 23(a)(1).** Consistent with Rule 23(a)(1), the members of the Class are so numerous and geographically dispersed that the joinder of all members is impractical. The Data Breach implicates at least 16,440 current and former KCC patients. KCC has physical and email addresses for Class members who therefore may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may include U.S. mail, electronic mail, internet postings, and/or published notice.

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

a. Whether KCC had a duty to protect patient PII;
b. Whether KCC knew or should have known of the susceptibility of its systems to a data breach;
c. Whether KCC's security measures to protect its systems were reasonable in light of best practices recommended by data security experts;
d. Whether KCC was negligent in failing to implement reasonable and adequate security procedures and practices;
e. Whether KCC's failure to implement adequate data security measures allowed the breach of its data systems to occur;
f. Whether KCC's conduct, including its failure to act, resulted in or was the proximate cause of the breach of its systems, resulting in the unlawful exposure of the Plaintiff's and Class Members' PII;
g. Whether Plaintiff and Class Members were injured and suffered damages or other losses because of KCC's failure to reasonably protect its systems and data network; and,

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

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

68. **Adequacy. Fed. R. Civ. P. 23(a)(4).** Consistent with Rule 23(a)(4), Plaintiff is an adequate representative of the Class because Plaintiff is a member of the Class he seeks to represent; is committed to pursuing this matter against KCC to obtain relief for the Class; and has no conflicts of interest with the Class. Moreover, Plaintiff's Counsel are competent and experienced in litigating class actions, including privacy litigation of this kind. Plaintiff intends to vigorously prosecute this case and will fairly and adequately protect the Class's interests.

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

70. **Injunctive and Declaratory Relief.** Class certification is also appropriate under Rule 23(b)(2) and (c). Defendant, through its uniform conduct, acted or refused to act on grounds

generally applicable to the Class as a whole, making injunctive and declaratory relief appropriate to the Class as a whole.

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

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

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

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

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

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

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

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

FIRST CAUSE OF ACTION
NEGLIGENCE
(On behalf of all Classes)

73. Plaintiff restates and realleges paragraphs 1 through 72 above as if fully set forth herein.

74. As a condition of receiving services, Plaintiff and Class Members were obligated to provide KCC, through their respective insurance carriers, with their PII.

75. Plaintiff and the Class Members entrusted their PII to KCC with the understanding that KCC would safeguard their information.

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

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

78. Plaintiff and the Class Members were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew of or should have known of the inherent risks in collecting and storing the PII of Plaintiff and the Class, the critical importance of providing adequate security of that PII, that it had inadequately trained and educated its employees, and that its security protocols were insufficient to secure the PII of Plaintiff and Class Members.

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

80. Plaintiff and the Class Members had no ability to protect their PII that was in KCC's possession.

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

82. Defendant had a duty to have proper procedures in place to prevent the unauthorized dissemination Plaintiff and Class Members' PII.

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

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

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

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

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

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

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

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

SECOND CAUSE OF ACTION
NEGLIGENCE PER SE
(On behalf of all Classes)

91. Plaintiff restates and realleges Paragraphs 1 through 72 as if fully set forth herein.

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

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

94. KCC's violation of Section 5 of the FTC Act constitutes negligence per se.

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

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

97. As a direct and proximate result of KCC's negligence per se, Plaintiff and the Class have suffered, and continue to suffer, injuries and damages.

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

THIRD CAUSE OF ACTION
INVASION OF PRIVACY
(On behalf of all Classes)

99. Plaintiff restates and realleges paragraphs 1 through 72 above as if fully set forth herein.

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

101. Defendant owed a duty to patients in its network, including Plaintiff and Class Members, to keep their PII contained as a part thereof, confidential.

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

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

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

105. Defendant acted with a knowing state of mind when it permitted the Data Breach because it had actual knowledge that its information security practices were inadequate.

106. Because Defendant acted with a knowing state of mind, it had notice and knew that its inadequate information security practices would cause injury and harm to Plaintiff and Class Members.

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

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

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

FOURTH CAUSE OF ACTION
BREACH OF IMPLIED CONTRACT
(On behalf of all Classes)

109. Plaintiff restates and realleges paragraphs 1 through 72 above as if fully set forth herein.

110. Plaintiff and Class Members were required to provide their PII, including names, addresses, dates of birth, Social Security numbers and various health related information to Defendant as a condition of their use of Defendant's services.

111. Plaintiff and Class Members paid money to Defendant in exchange for services, as well as Defendant's promises to protect their protected health information and other PII from unauthorized disclosure.

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

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

114. Implicit in the agreement between the Defendant's patients, including Plaintiff and Class Members, to provide protected health information and other PII, and Defendant's acceptance of such protected health information and other PII, was Defendant's obligation to use such PII for business purposes only, take reasonable steps to secure and safeguard that protected health information and other PII, and not make unauthorized disclosures of the protected health information and other PII to unauthorized third parties.

115. Further, implicit in the agreement, Defendant was obligated to provide Plaintiff and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their PII.

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

117. Defendant had an implied duty to reasonably safeguard and protect the PII of Plaintiff and Class Members from unauthorized disclosure or uses.

118. Additionally, Defendant implicitly promised to retain this PII only under conditions that kept such information secure and confidential.

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

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

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

b. failing to comply with their promise to abide by HIPAA.

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

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

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

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

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

FIFTH CAUSE OF ACTION
UNJUST ENRICHMENT
(On behalf of all Classes)

121. Plaintiff restates and realleges paragraphs 1 through 72 above as if fully set forth herein.

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

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

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

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

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

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

128. If Plaintiff and Class Members knew that Defendant would not secure its PII using adequate security measures, they would not have engaged in transactions with Defendant.

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

130. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft (ii) the compromise, publication, and/or theft of their PII; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their 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 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 such PII; and (vi) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

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

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

SIXTH CAUSE OF ACTION
BREACH OF FIDUCIARY DUTY
(On behalf of all Classes)

133. Plaintiff restates and realleges paragraphs 1 through 72 above as if fully set forth herein.

134. In light of the special relationship between Defendant and its patients, whereby Defendant became a guardian of Plaintiff's and Class Members' highly sensitive, confidential PII. Defendant became a fiduciary by its undertaking and guardianship of such PII, to act primarily for the benefit of its patients to: 1) safeguard Plaintiff and Class Members' PII; 2) timely notify Plaintiff

and Class Members' of a data breach or disclosure of such PII; and 3) maintain complete and accurate records of what and where patients information was and is stored.

135. Defendant has a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of its patients' relationship, in particular to keep secure the PII of its patients.

136. Defendant breached its fiduciary duties to Plaintiff and Class Members by:

a. failing to diligently investigate the Data Breach to determine the number of Class Members affected in a reasonable and practicable period of time.

b. failing to encrypt and otherwise protect the integrity of the system containing Plaintiff's and Class Members' protected health information and other PII.

c. failing to timely notify and/or warn Plaintiff and Class Members of the Data Breach.

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

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

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

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

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

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

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

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

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

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

n. otherwise failing to safeguard Plaintiff's and Class Members' PII.

137. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their PII; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their 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 PII, which remains in Defendant's

possession and is subject to further unauthorized disclosures so long as Defendant fail to undertake appropriate and adequate measures to protect Patient PII in their continued possession; and (vi) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

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

SEVENTH CAUSE OF ACTION
BREACH OF CONFIDENCE
(On behalf of all Classes)

139. Plaintiff restates and realleges paragraphs 1 through 70 above as if fully set forth herein.

140. At all times during Plaintiff's and Class Members' interactions with Defendant, Defendant was fully aware of the confidential and sensitive nature of Plaintiff's and Class Members' protected health information and other PII that Plaintiff and Class Members provided to Defendant.

141. As alleged herein and above, Defendant's relationship with Plaintiff and Class Members was governed by terms and expectations that Plaintiff's and Class Members' protected health information and other PII would be collected, stored, and protected in confidence, and would not be disclosed the unauthorized third parties.

142. Plaintiff and Class Members provided their respective protected health and personal information to Defendant with the explicit and implicit understanding that KCC would protect from and prevent the unauthorized dissemination of such PII.

143. Plaintiff and Class Members also provided their respective protected health information and PII to Defendant with the explicit and implicit understanding that Defendant would take precautions to protect that protected health information and other PII from unauthorized disclosure, such as following basic principles of encryption and information security practices.

144. Defendant voluntarily received in confidence Plaintiff's and Class Members' protected health information and other PII with the understanding that protected health information and other PII would not be disclosed or disseminated to the public or any unauthorized third parties.

145. Due to Defendant's failure to prevent, detect, avoid the Data Breach from occurring by, *inter alia*, following best information security practices to secure Plaintiff's and Class Members' protected health information and other PII, Plaintiff's and Class Members' protected health information and PII was disclosed and misappropriated to unauthorized third parties beyond Plaintiff's and Class Members' confidence, and without their express permission.

146. As a direct and proximate cause of Defendant's actions and/or omissions, Plaintiff and Class Members have suffered damages.

147. But for Defendant's disclosure of Plaintiff's and Class Members' protected health information and other PII in violation of the parties' understanding of confidence, their protected health information and other PII would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Defendant's Data Breach was the direct and legal cause of the theft of Plaintiff's and Class Members' protected health information and other PII, as well as the resulting damages.

148. The injury and harm Plaintiff and Class Members suffered was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiff's and Class Members' protected health information and other PII. Defendant knew their computer systems and technologies for accepting and securing Plaintiff's and Class Members' protected health information and other PII had numerous security vulnerabilities because Defendant failed to observe even basic security practices necessary to prevent fraudulent provider accounts from being created.

149. As a direct and proximate result of Defendant's breaches of confidence, Plaintiff 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 PII; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their 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 identity theft; (v) the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fail to undertake appropriate and adequate measures to protect Patient PII in their continued possession; and (vi) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

150. As a direct and proximate result of Defendant's breaches of confidence, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

EIGHT CUASE OF ACTION
KENTUCKY CONSUMER PROTECTION ACT,
Ky. Rev. Stat. §§ 367.110, *et seq.*
(On behalf of the Kentucky Subclass)

151. Plaintiff restates and realleges paragraphs 1 through 70 above as if fully set forth herein.

152. Plaintiff and Kentucky Subclass Members purchased goods and services for personal, family, and/or household purposes from KCC.

153. KCC, operating in Kentucky, engaged in deceptive, unfair, and unlawful trade acts or practices in the conduct of trade or commerce, in violation of Ky. Rev. Stat. § 367.170, including but not limited to the following:

a. Fraudulently advertising material facts pertaining to its good and services to the Kentucky Subclass by representing and advertising that it would maintain adequate data privacy and security practices and procedures to safeguard Kentucky Subclass Members' Personal Information from unauthorized disclosure, release, data breaches, and theft;

b. Misrepresenting material facts pertaining to goods and services to the Kentucky Subclass by representing and advertising that it did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Kentucky Subclass Members' Personal Information;

c. Omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security protections for Kentucky Subclass Members' Personal Information;

d. Engaging in deceptive, unfair, and unlawful trade acts or practices by failing to maintain the privacy and security of Kentucky Subclass Members' Personal Information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the Data Breach;

e. Engaging in deceptive, unfair, and unlawful trade acts or practices by failing to disclose the KCC Data Breach to Kentucky Subclass Members in a timely and accurate manner, contrary to the duties imposed by Ky. Rev. Stat. § 365.732(2); and

f. Engaging in deceptive, unfair, and unlawful trade acts or practices by failing to take proper action following the KCC Data Breach to enact adequate privacy and security measures and protect Kentucky Subclass Members' Personal Information from further unauthorized disclosure, release, data breaches, and theft.

154. As a direct and proximate result of KCC's deceptive trade practices, Kentucky Subclass Members suffered an ascertainable loss of money or property, real or personal, as described above, including the loss of their legally protected interest in the confidentiality and privacy of their Personal Information.

155. The above unfair and deceptive practices and acts by KCC were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and Kentucky

Subclass Members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

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

157. KCC knew or should have known that its computer systems and data security practices were inadequate to safeguard Kentucky Subclass Members' Personal Information and that the risk of a data breach or theft was high. KCC's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the Kentucky Subclass.

158. Plaintiff and Kentucky Subclass Members seek relief under Ky. Rev. Stat. § 367.220, including, but not limited to, damages, punitive damages, restitution and/or other equitable relief, injunctive relief, and/or attorneys' fees and costs.

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

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

b. An Order appointing Plaintiff as the class representative;

c. An Order appointing undersigned counsel as class counsel;

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

e. An award of damages;

f. An award of costs and expenses;

g. An award of attorneys' fees; and

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

DEMAND FOR JURY TRIAL

Plaintiffs demand a jury trial as to all issues triable by a jury.

.

Dated: October 2, 2019

Respectfully Submitted,

/s/ Brenton D. Stanley
Brenton D. Stanley, KBA # 94925
MORGAN & MORGAN KENTUCKY, PLLC
420 West Liberty Street, Suite 260
Louisville, KY 40202-3048
(502) 912-5906 Telephone
bstanley@forthepeople.com

John A. Yanchunis (*Pro Hac Vice to be submitted)*
jyanchunis@ForThePeople.com
Patrick A. Barthle (*Pro Hac Vice to be submitted)*
pbarthle@forthepoeple.com
MORGAN & MORGAN
COMPLEX LITIGATION GROUP
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
Telephone: (813) 223-5505
Facsimile: (813) 223-5402

Counsel for Plaintiffs

Kentucky Counseling Center
Return Mail Processing Center
PO Box 6336
Portland, OR 97228-6336

413700070965
000 0002191 00000000 0001 0002 01096 INS: 0 0
CHRISTIAN SMITH
[redacted]

February 8, 2019

Dear Christian Smith:

I am writing to make you aware of a recent incident at Kentucky Counseling Center (KCC). On January 4, 2019, a former KCC staff member reported receiving an email containing a link to a KCC patient list. KCC then began an investigation into the former staff member's report. Based on our investigation to date, we believe a KCC staff member took the list without authorization from our computer system on December 6, 2018. We believe that same individual used an anonymous Internet file sharing service to email the list to the former KCC staff member. The individual we believe to be responsible for the email is no longer working with KCC.

You are receiving this letter because you were included on the patient list mentioned above. While we do not believe the individual took the patient list to cause harm to individuals on the list, we wanted to make you aware of these circumstances out of an abundance of caution.

The type of information on the list varied for different people, but may have included the following: name; address; date of birth; email; phone number; Social Security Number; sex; marital and employment status; insurance payer and insurance number. The list did not include any clinical information other than the date of the last and/or next appointment for some individuals; and, in some cases, the names of KCC clinicians involved in an individual's care.

We have taken a number of steps to prevent this type of event from happening in the future, including strengthening our password requirements and requiring KCC staff members to provide a separate form of authentication, in addition to a username and password, to access our computer system.

We recommend you remain vigilant to the possibility of fraud and identity theft by reviewing account statements and monitoring free credit reports for unauthorized activity. To assist you, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (*my*TrueIdentity) for one year provided by TransUnion Interactive, a subsidiary of TransUnion®. TransUnion is one of the three nationwide credit reporting companies. Additional information on the *my*TrueIdentity service and the steps to follow for enrollment are enclosed with this letter. You may also obtain information for a free copy of your credit report from the three nationwide credit reporting agencies using the contact information below:

Equifax
P.O. Box 740241
Atlanta, GA 30374
www.equifax.com
1-800-685-1111

Experian
P.O. Box 2002
Allen, TX 75013
www.experian.com
1-888-397-3742

TransUnion
P.O. Box 1000
Chester, PA 19016
www.transunion.com
1-800-888-4213

If you suspect theft of your identity has occurred, you should contact your local law enforcement authorities to file a police report. You can also contact the Federal Trade Commission or your state Attorney General. The Federal Trade Commission provides information on steps an individual can take to avoid identity theft. You can also obtain additional information from the credit reporting agencies above or the Federal Trade Commission about placing a fraud alert or security freeze on your credit reports. Contact information for the Federal Trade Commission is:

Federal Trade Commission
600 Pennsylvania Ave.
Washington, DC 20580
www.ftc.gov/idtheft
1-877-438-4338

We sincerely regret that this event occurred and we have established a toll-free number for you to call, Monday through Friday from 9:00 AM to 9:00 PM Eastern Time, if you have questions. The toll-free number to call with questions is 877-431-9928.

Sincerely,

Matt Grammer
Owner, CEO
Kentucky Counseling Center

TransUnion

Activation Code: [redacted]

Complimentary One-Year *my*TrueIdentity Credit Monitoring Service

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (*my*TrueIdentity) for one year provided by TransUnion Interactive, a subsidiary of TransUnion,® one of the three nationwide credit reporting companies.

How to Enroll: You can sign up online or via U.S. mail delivery

- To enroll in this service, go to the myTrueIdentity website at **www.MyTrueIdentity.com** and, in the space referenced as "Enter Activation Code," enter the 12-letter Activation Code [redacted] and follow the three steps to receive your credit monitoring service online within minutes.
- If you do not have access to the Internet and wish to enroll in a similar off line, paper-based credit monitoring service, via U.S. mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at **1-855-288-5422**. When prompted, enter the six-digit telephone passcode **697168** and follow the steps to enroll in the off line credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

You can sign up for the online or off line credit monitoring service anytime between now and **May 31, 2019**. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH COMPLIMENTARY CREDIT MONITORING SERVICE:

- Once you are enrolled, you will be able to obtain one year of unlimited access to your TransUnion credit report and credit score.
- The daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion, including fraud alerts, new inquiries, new accounts, new public records, late payments, changes of address, and more.
- The service also includes access to an identity restoration program that provides assistance in the event that your identity is compromised and up to $1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

W9543 v.02 02.06.2019

JS 44 (Rev. 09/19)

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

CHRISTIAN SMITH. on behalf of himself and all others similarly situated,

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

(c) Attorneys *(Firm Name, Address, and Telephone Number)*
MORGAN & MORGAN KENTUCKY, PLLC
420 West Liberty Street, Suite 260
Louisville, KY 40202-3048

DEFENDANTS

KENTUCKY COUNSELING CENTER, 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

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

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

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

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

PROPERTY RIGHTS
- ☐ 820 Copyrights
- ☐ 830 Patent
- ☐ 835 Patent - Abbreviated New Drug Application
- ☐ 840 Trademark

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

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)***:
Class Action Fairness Act, 28 U.S.C. § 1332(d)(2)

Brief description of cause:
Negligence, Negligence per se, Invasion of Privacy, Breach of Implied Contract, Unjust Enrichment, et al.

VII. REQUESTED IN COMPLAINT:

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

DEMAND $ 5,000,000.00

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

VIII. RELATED CASE(S) IF ANY

(See instructions): JUDGE _____ DOCKET NUMBER _____

DATE
10/02/2019

SIGNATURE OF ATTORNEY OF RECORD
/s/ Brenton D. Stanley

FOR OFFICE USE ONLY

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