EFILED
4/11/2025 3:13 PM
Joseph B. Roesch
7th Judicial Circuit
Sangamon County, IL
2024LA000198

IN THE CIRCUIT COURT OF SANGAMON COUNTY ILLINOIS COUNTY DEPARTMENT, CHANCERY DIVISION

AARON UMBERGER and TRACY BRUNER, on behalf of themselves and all others similarly situated, Plaintiffs, v. **KERBER, ECK, & BRAECKEL LLP,** Defendant.	Case No. 2024LA000198 Honorable Judge Robert Hall **DEMAND FOR JURY TRIAL**

AMENDED CLASS ACTION COMPLAINT

Plaintiffs Aaron Umberger and Tracy Bruner ("Plaintiffs") individually and on behalf of all similarly situated persons, allege the following against Kerber, Eck, and Braeckel LLP ("KEB" or "Defendant") based upon personal knowledge with respect to themselves and on information and belief derived from, among other things, investigation by Plaintiffs' counsel and review of public documents as to all other matters:

I. INTRODUCTION

1. Plaintiffs bring this class action against KEB for its failure to properly secure and safeguard Plaintiffs' and other similarly situated KEB customers' patients' personally identifiable information ("PII") and protected health information ("PHI"), including name, address, date of birth, Social Security number, financial account information, Medical information (including but not limited to Diagnosis, Diagnosis Code, Mental/Physical Condition, Prescription information, and provider's name and location), Health insurance information (including but not limited to beneficiary number, subscriber number, Medicaid/Medicare identification), and/or Billing and

Claims information (including but not limited to patient account number, patient identification number, and treatment cost information) (the "Private Information"), from criminal hackers.

2. KEB, based in Springfield, Illinois, is a certified public accounting firm that provides a full range of accounting, tax, management consulting, and wealth management services to a diverse base of clients across the Midwest and the United States, including healthcare providers.

3. On or about August 12, 2024, KEB filed official notice of a hacking incident with the Attorney General of Massachusetts. Under state and federal law, organizations must report breaches involving PHI within at least sixty (60) days.

4. On or about the same day, KEB also sent out data breach letters (the "Notice") to individuals whose information was compromised as a result of the hacking incident.[1]

5. Based on the Notice sent to Plaintiffs and "Class Members" (defined below), unusual activity was detected on some of its computer systems around February 7, 2023.[2] In response, Defendant launched an investigation which revealed that an unauthorized party had access to certain files that contained sensitive information, and that such access took place between January 27 and February 7, 2023 (the "Data Breach").[3] Yet, KEB waited over a year to notify Plaintiffs and other Class Members that they were at risk.[4]

6. As a result of this delayed response, Plaintiffs and Class Members had no idea for over a year's time that their Private Information had been compromised, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm. The risk will remain for their respective lifetimes.

[1] Defendant's Notice addressed to Plaintiff Bruner is attached hereto as Exhibit A.
[2] *Id*.
[3] *Id*.
[4] *Id*.

7. The Private Information compromised in the Data Breach contained highly sensitive patient data, representing a gold mine for data thieves. The data included, but is not limited to, Social Security Numbers, medical information, health insurance information, and financial account information that KEB collected and maintained from its customers' patients.

8. Armed with the Private Information accessed in the Data Breach (and a head start), data thieves can commit a variety of crimes including, *e.g.*, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' names to obtain medical services, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

9. There has been no assurance offered by KEB that all personal data or copies of data have been recovered or destroyed, or that Defendant has adequately enhanced its data security practices sufficient to avoid a similar breach of its network in the future.

10. Therefore, Plaintiffs and Class Members have suffered and are at an imminent, immediate, and continuing increased risk of suffering, ascertainable losses in the form of harm from identity theft and other fraudulent misuse of their Private Information, the loss of the benefit of their bargain, out-of-pocket expenses incurred to remedy or mitigate the effects of the Data Breach, and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach.

11. Plaintiffs bring this class action lawsuit to address KEB's inadequate safeguarding of Class Members' Private Information that it collected and maintained, and its failure to provide

timely and adequate notice to Plaintiffs and Class Members of the types of information that were accessed, and that such information was subject to unauthorized access by cybercriminals.

12. The potential for improper disclosure and theft of Plaintiffs' and Class Members' Private Information was a known risk to KEB, and thus KEB was on notice that failing to take necessary steps to secure the Private Information left it vulnerable to an attack.

13. Upon information and belief, KEB failed to properly implement security practices with regard to the computer network and systems that housed the Private Information. Had KEB properly monitored its networks, it would have discovered the Breach sooner.

14. Plaintiffs' and Class Members' identities are now at risk because of KEB's negligent conduct as the Private Information that KEB collected and maintained for s customers is now in the hands of data thieves and other unauthorized third parties.

15. Plaintiffs seek to remedy these harms on behalf of themselves and all similarly situated individuals whose Private Information was accessed and/or compromised during the Data Breach.

16. Accordingly, Plaintiffs, on behalf of themselves and the Class, assert claims for negligence, negligence *per se*, breach of implied contract, unjust enrichment, breach of fiduciary duty, breach of confidence, breach of third-party beneficiary contract, and declaratory judgment this Court deems appropriate.

II. PARTIES

17. Plaintiff Aaron Umberger is, and at all times mentioned herein was, an individual citizen of the State of Illinois, residing in Edgar County.

18. Plaintiff Tracy Bruner is, and at all times mentioned herein was, an individual citizen of the State of Illinois, residing in Lawrence County.

19. Defendant KEB is a public accounting firm incorporated in Illinois with its principal place of business at 322 Robbins Rd. Ste. 200A, Springfield, Illinois 62704 in Sangamon County.

III. JURISDICTION AND VENUE

20. This Court has subject matter jurisdiction pursuant to 735 ILCS 5/2-209.

21. This Court has personal jurisdiction over Defendant because Defendant maintains its principal place of business in Springfield, Illinois in Sangamon County. Furthermore, Defendant intentionally availed itself of this jurisdiction by marketing, employing individuals, and providing accounting services in Illinois.

22. Venue is proper in this Court pursuant to 735 ILCS 5/2-101 because Defendant operates in this County and a substantial part of the events, acts, and omissions giving rise to Plaintiffs' claims occurred in this County.

IV. FACTUAL ALLEGATIONS

A. KEB's Business and Collection of Plaintiffs' and Class Members' Private Information

23. Founded in 1938, KEB is a public accounting firm whose services expand beyond traditional audit, accounting and tax preparation services to include management and financial consulting, investigative accounting, litigation support, business valuation, employee benefit plans and administration, financial planning and wealth management. KEB currently has 27 partners/principals and over 190 professionals across 5 office groups in three states.

24. As a condition of receiving these services, KEB requires that its healthcare customers entrust it with their patients' highly sensitive personal and health information. In the ordinary course of receiving service from KEB, healthcare customers were required to provide their patients', like Plaintiffs and Class Members, Private Information to Defendant.

25. In its Notice of Privacy Practices, KEB promises its customers that "[t]he Firm takes your privacy very seriously"[5] and says that "We share a commitment to protect your privacy and the confidentiality of your personal financial information. The Firm applies professional standards of confidentiality that are even more stringent than those required by law. Therefore, protecting the confidentiality of that information has been, and will continue to be, a top priority for the Firm."[6]

26. Thus, due to the highly sensitive and personal nature of the information KEB acquires and stores with respect to its healthcare customers' patients, KEB, upon information and belief, promises to, among other things: keep patients' Private Information private; comply with industry standards related to data security and the maintenance of its customers' patients' Private Information; inform its customers' patients of its legal duties relating to data security and comply with all federal and state laws protecting customers' patients' Private Information; only use and release customers' patients' Private Information for reasons that relate to the services it provides; and provide adequate notice to customers' patients if their Private Information is disclosed without authorization.

27. By obtaining, collecting, using, and deriving a benefit from its health customers' patients Private Information, KEB assumed legal and equitable duties it owed to them and knew or should have known that it was responsible for protecting Plaintiffs' and Class Members' Private Information from unauthorized disclosure and exfiltration.

[5] https://kebcpa.com/privacy-policy/ (Last visited Aug. 20, 2024).

[6] *Id*.

28. Plaintiffs and Class Members relied on KEB to keep their Private Information confidential and securely maintained and to only make authorized disclosures of this Information, which Defendant ultimately failed to do.

B. The Data Breach and Defendant's Inadequate Notice to Plaintiffs and Class Members

29. According to Defendant's Notice, it learned of unauthorized access to its computer systems on February 7, 2023, with such unauthorized access having taken place between January 27 and February 7, 2023.[7]

30. Through the Data Breach, the unauthorized cybercriminal(s) accessed a cache of highly sensitive Private Information, including name, address, date of birth, Social Security number, financial account information, Medical information (including but not limited to Diagnosis, Diagnosis Code, Mental/Physical Condition, Prescription information, and provider's name and location), Health insurance information (including but not limited to beneficiary number, subscriber number, Medicaid/Medicare identification), and/or Billing and Claims information (including but not limited to patient account number, patient identification number, and treatment cost information).

31. On or about August 12, 2024, roughly 18 months after KEB learned that the Class's Private Information was first accessed by cybercriminals, KEB finally began to notify Plaintiffs and other Class Members that its investigation determined that their Private Information was impacted.[8]

32. KEB had obligations created by contract, industry standards, common law, and representations made to Plaintiffs and Class Members to keep Plaintiffs' and Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

[7] Ex. A.
[8] *Id.*

33. Plaintiffs and Class Members provided their Private Information to KEB with the reasonable expectation and mutual understanding that KEB would comply with its obligations to keep such Information confidential and secure from unauthorized access and to provide timely notice of any security breaches.

34. KEB's data security obligations were particularly important given the substantial increase in cyberattacks in recent years.

35. KEB knew or should have known that its electronic records would be targeted by cybercriminals.

C. The Healthcare Sector is Particularly Susceptible to Data Breaches

36. KEB was on notice that its customers' patients' data is a target for data breaches.

37. KEB was also on notice that the FBI has been concerned about data security in the healthcare industry. In August 2014, after a cyberattack on Community Health Systems, Inc., the FBI warned companies involved 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 (PHI)."[9]

38. 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

[9] Jim Finkle, *FBI Warns Healthcare Firms that they are Targeted by Hackers*, Reuters (Aug. 2014), *available at* https://www.reuters.com/article/us-cybersecurity-healthcare-fbi/fbi-warns-healthcare-firms-they-are-targeted-by-hackers-idUSKBN0GK24U20140820 (last visited on Aug. 20, 2024).

> patients' health and financial information, but also patient access to care.[10]

39. The healthcare sector reported the second largest number of data breaches among all measured sectors in 2018, with the highest rate of exposure per breach.[11] In 2022, the largest growth in compromises occurred in the healthcare sector.[12]

40. Indeed, when compromised, healthcare related data is among the most sensitive and personally consequential. A report focusing on healthcare breaches found that the "average total cost to resolve an identity theft-related incident … came to about $20,000," and that the victims were often forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[13]

41. Almost 50 percent of the victims lost their healthcare coverage as a result of the incident, while nearly 30 percent said their insurance premiums went up after the event. Forty percent of the customers were never able to resolve their identity theft at all. Data breaches and identity theft have a crippling effect on individuals and detrimentally impact the economy as a whole.[14]

---

[10] Andis Robeznieks, *Cybersecurity: Ransomware attacks shut down clinics, hospitals*, Am. Med. Ass'n. (Oct. 4, 2019), *available at*: https://www.ama-assn.org/practice-management/sustainability/cybersecurity-ransomware-attacks-shut-down-clinics-hospitals (last visited on Aug. 20, 2024).

[11] Identity Theft Resource Center, *2018 End-of-Year Data Breach Report, available at*: https://www.idtheftcenter.org/2018-data-breaches/ (last visited on Aug. 20, 2024).

[12] Identity Theft Resource Center, *2022 End-of-Yeare Data Breach Report, available at*: https://www.idtheftcenter.org/wp-content/uploads/2023/01/ITRC_2022-Data-Breach-Report_Final-1.pdf (last visited on Aug. 20, 2024).

[13] Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (March 3, 2010), *available at:* https://www.cnet.com/news/privacy/study-medical-identity-theft-is-costly-for-victims/ (last visited on Aug. 20, 2024).

[14] *Id*.

42. Healthcare related breaches have continued to rapidly increase because electronic patient data is seen as a valuable asset. "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."[15]

43. As an accounting provider for the healthcare industry, KEB knew, or should have known, the importance of safeguarding its customers' patients' Private Information, including PHI, entrusted to it, and of the foreseeable consequences if such data were to be disclosed. These consequences include the significant costs that would be imposed on KEB's customers' patients as a result of a breach. KEB failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring.

D. KEB's Negligence is Evidenced by its Failure to Comply with HIPAA

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

45. KEB's Data Breach resulted from a combination of insufficiencies that indicate KEB failed to comply with safeguards mandated by HIPAA regulations and industry standards. First, it can be inferred from KEB's Data Breach that KEB either failed to implement, or

[15] Inside Digital Health, *How to Safeguard Hospital Data from Email Spoofing Attacks*, April 4, 2019, *available at*: https://www.chiefhealthcareexecutive.com/view/how-to-safeguard-hospital-data-from-email-spoofing-attacks (last visited on Aug. 20, 2024).

inadequately implemented, information security policies or procedures to protect Plaintiffss and Class Members' PHI.

46. Plaintiffs' and Class Members' Private Information compromised in the Data Breach included "protected health information" as defined by CFR § 160.103.

47. 45 CFR § 164.402 defines "breach" as "the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information."

48. 45 CFR § 164.402 defines "unsecured protected health information" as "protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the [HHS] Secretary[.]"

49. Plaintiffs' and Class Members' Private Information included "unsecured protected health information" as defined by 45 CFR § 164.402.

50. Plaintiffs' and Class Members' unsecured PHI was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E, as a result of the Data Breach.

51. Based upon Defendant's Notice to Plaintiffs and Class Members, KEB reasonably believes that Plaintiffs' and Class Members' unsecured PHI has been acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E, as a result of the Data Breach.

52. Plaintiffs' and Class Members' unsecured PHI that was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach was not rendered unusable, unreadable, or indecipherable to unauthorized persons.

53. KEB reasonably believes that Plaintiffs' and Class Members' unsecured PHI that was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart

E as a result of the Data Breach was not rendered unusable, unreadable, or indecipherable to unauthorized persons.

54. Plaintiffs' and Class Members' unsecured PHI that was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach, and which was not rendered unusable, unreadable, or indecipherable to unauthorized persons, was viewed by unauthorized persons.

55. Plaintiffs' and Class Members' unsecured PHI was viewed by unauthorized persons in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach.

56. KEB reasonably believes that Plaintiffs' and Class Members' unsecured PHI was viewed by unauthorized persons in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach.

57. It is reasonable to infer that Plaintiffs' and Class Members' unsecured PHI that was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach, and which was not rendered unusable, unreadable, or indecipherable to unauthorized persons, was viewed by unauthorized persons.

58. It should be rebuttably presumed that unsecured PHI acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E, and which was not rendered unusable, unreadable, or indecipherable to unauthorized persons, was viewed by unauthorized persons.

59. After receiving notice that they were victims of the Data Breach (which required the filing of a data breach report in accordance with 45 CFR § 164.408(a)), it is reasonable for recipients of that notice, including Plaintiffs and Class Members in this case, to believe that future

harm (including medical identity theft) is real and imminent, and to take steps necessary to mitigate that risk of future harm.

60. In addition, KEB's Data Breach could have been prevented if KEB had implemented HIPAA mandated, industry standard policies and procedures for securely disposing of PHI when it was no longer necessary and/or had honored its obligations to its customers' patients.

61. KEB's security failures also include, but are not limited to:

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

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

c. Failing to ensure the confidentiality and integrity of electronic protected health information KEB creates, receives, maintains, and transmits in violation of 45 CFR 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 CFR 164.312(a)(1);

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

f. Failing to identify and respond to suspected or known security incidents;

g. Failing to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity, in violation of 45 CFR 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 CFR 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 CFR 164.306(a)(3);

j. Failing to ensure compliance with HIPAA security standard rules by Defendant's workforce, in violation of 45 CFR 164.306(a)(94); and

k. Impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons, in violation of 45 CFR 164.502, *et seq.*

62. The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414 also required KEB to provide notice of the Data Breach to each affected individual "without unreasonable delay and ***in no case later than 60 days following discovery of the breach***" (emphasis added). KEB also failed in this regard.

E. KEB Failed to Comply with FTC Guidelines

63. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision making. Indeed, the FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in

violation of Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

64. In October 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep, properly dispose of personal information that is no longer needed, encrypt information stored on computer networks, understand their network's vulnerabilities, and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs, monitor all incoming traffic for activity indicating someone is attempting to hack into the system, watch for large amounts of data being transmitted from the system, and have a response plan ready in the event of a breach.

65. The FTC further 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 the network for suspicious activity, and verify that third-party service providers have implemented reasonable security measures.

66. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data by 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 the FTCA. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

67. As evidenced by the Data Breach, KEB failed to properly implement basic data security practices. KEB's failure to employ reasonable and appropriate measures to protect against

unauthorized access to Plaintiffs' and Class Members' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

68. KEB was at all times fully aware of its obligation to protect the Private Information of its customers' patients yet failed to comply with such obligations. Defendant was also aware of the significant repercussions that would result from its failure to do so.

F. KEB Failed to Comply with Industry Standards

69. As noted above, experts studying cybersecurity routinely identify businesses as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

70. Some industry best practices that should be implemented by businesses dealing with sensitive PHI like KEB include but are not limited to: educating all employees, strong password requirements, multilayer security including firewalls, anti-virus and anti-malware software, encryption, multi-factor authentication, backing up data, and limiting which employees can access sensitive data. As evidenced by the Data Breach, Defendant failed to follow some or all of these industry best practices.

71. Other best cybersecurity practices that are standard in the industry include: installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protecting physical security systems; and training staff regarding these points. As evidenced by the Data Breach, Defendant failed to follow these cybersecurity best practices.

72. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation

PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

73. Defendant failed to comply with these accepted standards, thereby permitting the Data Breach to occur.

G. KEB Breached its Duty to Safeguard Plaintiffs' and Class Members' Private Information

74. In addition to its obligations under federal and state laws, KEB owed a duty to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. KEB owed a duty to Plaintiffs and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected the Private Information of Class Members

75. KEB breached its obligations to Plaintiffs and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data. KEB's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system that would reduce the risk of data breaches and cyberattacks;

b. Failing to adequately protect customers' patients' Private Information;

c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to sufficiently train its employees regarding the proper handling of its customers' patients Private Information;

e. Failing to fully comply with FTC guidelines for cybersecurity in violation of the FTCA;

f. Failing to adhere to HIPAA and industry standards for cybersecurity as discussed above; and

g. Otherwise breaching its duties and obligations to protect Plaintiffs' and Class Members' Private Information.

76. KEB negligently and unlawfully failed to safeguard Plaintiffs' and Class Members' Private Information by allowing cyberthieves to access its computer network and systems which contained unsecured and unencrypted Private Information.

77. Had KEB remedied the deficiencies in its information storage and security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, it could have prevented intrusion into its information storage and security systems and, ultimately, the theft of Plaintiffs' and Class Members' confidential Private Information.

78. Accordingly, Plaintiffs' and Class Members' lives were severely disrupted. What's more, they have been harmed as a result of the Data Breach and now face an increased risk of future harm that includes, but is not limited to, fraud and identity theft. Plaintiffs and Class Members also lost the benefit of the bargain they made with customers of KEB.

H. KEB Should Have Known that Cybercriminals Target PII and PHI to Carry Out Fraud and Identity Theft

79. The FTC hosted a workshop to discuss "informational injuries," which are injuries that consumers like Plaintiffs and Class Members suffer from privacy and security incidents such

as data breaches or unauthorized disclosure of data.[16] Exposure of highly sensitive personal information that a consumer wishes to keep private may cause harm to the consumer, such as the ability to obtain or keep employment. Consumers' loss of trust in e-commerce also deprives them of the benefits provided by the full range of goods and services available which can have negative impacts on daily life.

80. Any victim of a data breach is exposed to serious ramifications regardless of the nature of the data that was breached. Indeed, the reason why criminals steal information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims or to take over victims' identities in order to engage in illegal financial transactions under the victims' names.

81. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity or to otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

82. In fact, as technology advances, computer programs may scan the Internet with a wider scope to create a mosaic of information that may be used to link compromised information to an individual in ways that were not previously possible. This is known as the "mosaic effect."

[16] *FTC Information Injury Workshop, BE and BCP Staff Perspective,* Federal Trade Commission, (October 2018), *available at* https://www.ftc.gov/system/files/documents/reports/ftc-informational-injury-workshop-be-bcp-staff-perspective/informational_injury_workshop_staff_report_-_oct_2018_0.pdf (last visited on Aug. 20, 2024).

Names and dates of birth, combined with contact information like telephone numbers and email addresses, are very valuable to hackers and identity thieves as it allows them to access users' other accounts.

83. Thus, even if certain information was not purportedly involved in the Data Breach, the unauthorized parties could use Plaintiffs' and Class Members' Private Information to access accounts, including, but not limited to, email accounts and financial accounts, to engage in a wide variety of fraudulent activity against Plaintiffs and Class Members.

84. One such example of this is the development of "Fullz" packages.

85. Cybercriminals can cross-reference two sources of the Private Information compromised in the Data Breach to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

86. The development of "Fullz" packages means that the stolen Private Information from the Data Breach can easily be used to link and identify it to Plaintiffs' and the proposed Class's phone numbers, email addresses, and other sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card or financial account numbers may not be included in the Private Information stolen in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiffs and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiffs and other Class Members' stolen Private Information is being misused, and that such misuse is fairly traceable to the Data Breach.

87. For these reasons, the FTC recommends that identity theft victims take several time-consuming steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert on their account (and an extended fraud alert that lasts for 7 years if someone steals the victim's identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a freeze on their credit, and correcting their credit reports.[17] However, these steps do not guarantee protection from identity theft but can only mitigate identity theft's long-lasting negative impacts.

88. Identity thieves can also use stolen personal information such as Social Security numbers and PHI for a variety of crimes, including credit card fraud, phone or utilities fraud, bank fraud, to obtain a driver's license or official identification card in the victim's name but with the thief's picture, to obtain government benefits, or to file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house in the victim's name, receive medical services in the victim's name, and even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

89. PHI is also especially valuable to identity thieves. As the FTC recognizes, identity thieves can use PHI to commit an array of crimes, including identity theft and medical and financial fraud.[18]

90. Indeed, a robust cyber black market exists in which criminals openly post stolen PHI on multiple underground Internet websites, commonly referred to as the dark web.

---

[17] *See IdentityTheft.gov,* Federal Trade Commission, *available at* https://www.identitytheft.gov/Steps (last visited Aug. 20, 2024).

[18] Federal Trade Commission, *Warning Signs of Identity Theft, available at*: https://consumer.ftc.gov/articles/what-know-about-identity-theft (last visited on Aug. 20, 2024).

91. While credit card information and associated PII can sell for as little as $1-$2 on the black market, protected health information can sell for as much as $363 according to the Infosec Institute.[19]

92. PHI is particularly valuable because criminals can use it to target victims with frauds and scams that take advantage of the victim's medical conditions or victim settlements. It can be used to create fake insurance claims, allowing for the purchase and resale of medical equipment, or gain access to prescriptions for illegal use or resale.

93. Medical identity theft can result in inaccuracies in medical records and costly false claims. It can also have life-threatening consequences. If a victim's health information is mixed with other records, it can lead to misdiagnosis or mistreatment. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[20]

94. The ramifications of KEB's failure to keep its customers' patients' Private Information secure are long lasting and severe. Once it is stolen, fraudulent use of such and damage to victims may continue for years.

95. Here, not only was sensitive medical information compromised, but financial information and Social Security numbers were compromised too. The value of both PII and PHI is axiomatic. The value of "big data" in corporate America is astronomical. The fact that identity

[19] Center for Internet Security, *Data Breaches: In the Healthcare Sector, available at*: https://www.cisecurity.org/insights/blog/data-breaches-in-the-healthcare-sector (last visited on Aug. 20, 2024).

[20] Michael Ollove, "The Rise of Medical Identity Theft in Healthcare," Kaiser Health News, Feb. 7, 2014, *available at*: https://kffhealthnews.org/news/rise-of-indentity-theft/ (last visited on Aug. 20, 2024).

thieves attempt to steal identities notwithstanding possible heavy prison sentences illustrates beyond a doubt that the Private Information compromised here has considerable market value.

96. It must also be noted that there may be a substantial time lag between when harm occurs and when it is discovered, and also between when PII and/or PHI is stolen and when it is misused. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:[21]

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

97. PII and PHI are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the dark web for years.

98. As a result, Plaintiffs and Class Members are at an increased risk of fraud and identity theft, including medical identity theft, for many years into the future. Thus, Plaintiffs and Class Members have no choice but to vigilantly monitor their accounts for many years to come.

I. Plaintiffs' and Class Members' Damages

Plaintiff Aaron Umberger's Experience

99. Plaintiff Umberger was a patient of Hospital and Medical Foundation of Paris, Inc. d/b/a Horizon Health, a customer of KEB.

[21] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO (June 2007), *available at* https://www.gao.gov/assets/270/262904.html (last visited Aug. 20, 2024).

100. When Horizon Health became a customer of KEB, Defendant required Horizon Health provide it with substantial amounts of Plaintiff Umberger's Private Information, including PHI.

101. On or about August 12, 2024, Plaintiff Umberger received a letter entitled "Notice of security Incident" which told him that his Private Information had been impacted during the Data Breach. The notice letter informed him that the Private Information stolen included his "billing/claim information, patient identification number, and treatment information".

102. The notice letter offered Plaintiff Umberger only provided Plaintiff with steps he can take to protect himself. This is not sufficient given that Plaintiff will now experience a lifetime of increased risk of identity theft, including but not limited to, potential medical fraud.

103. Plaintiff Umberger suffered actual injury in the form of time spent dealing with the Data Breach and the increased risk of fraud resulting from the Data Breach and/or monitoring his accounts for fraud.

104. Plaintiff Umberger would not have provided his Private Information to Horizon Health or Defendant had Defendant timely disclosed that its systems lacked adequate computer and data security practices to safeguard its customers' patients' personal and health information from theft, and that those systems were subject to a data breach.

105. Plaintiff Umberger suffered actual injury in the form of having his PII and PHI compromised and/or stolen as a result of the Data Breach, supported by a recent notification that his email was now on the dark web.

106. Plaintiff Umberger suffered actual injury in the form of damages to and diminution in the value of his personal, health, and financial information – a form of intangible property that

Plaintiff and Horizon Health entrusted to Defendant for the purpose of receiving accounting services from Defendant and which was compromised in, and as a result of, the Data Breach.

107. Plaintiff Umberger suffered imminent and impending injury arising from the substantially increased risk of future fraud, identity theft, and misuse posed by his Private Information being placed in the hands of criminals.

108. Plaintiff Umberger has a continuing interest in ensuring that his PII and PHI, which remain in the possession of Defendant, are protected and safeguarded from future breaches.

109. As a result of the Data Breach, Plaintiff Umberger made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach and reviewing financial accounts for any indications of actual or attempted identity theft or fraud. Plaintiff has spent several hours dealing with the Data Breach, valuable time he otherwise would have spent on other activities.

110. As a result of the Data Breach, Plaintiff Umberger has suffered anxiety as a result of the release of his PII and PHI, which he believed would be protected from unauthorized access and disclosure. These feelings include anxiety about unauthorized parties viewing, selling, and/or using his PII and PHI for purposes of committing cyber and other crimes against his including, but not limited to, fraud and identity theft. Plaintiff is very concerned about this increased, substantial, and continuing risk, as well as the consequences that identity theft and fraud resulting from the Data Breach would have on his life.

Plaintiff Tracy Bruner's Experience

111. Plaintiff Bruner was a patient of Harrisburg Medical Center ("Harrisburg"), a customer of KEB.

112. When Harrisburg became a customer of KEB, Defendant required Harrisburg provide it with substantial amounts of Plaintiff Bruner's Private Information, including PHI.

113. On or about August 2024, Plaintiff Bruner received a letter entitled "Notice of Security Incident" which informed Plaintiff that her Private Information had been impacted during the Data Breach.[22] The notice letter informed her that the Private Information stolen included her:

a. name;

b. date of birth;

c. medical record number; and,

d. treatment information.[23]

114. Defendant's Breach Notice only provided Plaintiff Bruner with steps she could take to protect herself.[24] This is not sufficient given that Plaintiff will now experience a lifetime of increased risk of identity theft, including but not limited to, potential medical fraud.

115. Plaintiff Bruner suffered actual injury in the form of time spent dealing with the Data Breach and the increased risk of fraud resulting from the Data Breach and/or monitoring her accounts for fraud.

116. Plaintiff Umberger would not have provided her Private Information to Harrisburg or Defendant had Defendant timely disclosed that its systems lacked adequate computer and data security practices to safeguard its customers' patients' personal and health information from theft, and that those systems were subject to a data breach.

[22] Ex. A.
[23] *Id*.
[24] *See id*.

117. Plaintiff Bruner suffered actual injury in the form of having her PII and PHI compromised and/or stolen as a result of the Data Breach, supported by a dramatic increase in medical-related spam calls she has experienced.

118. Plaintiff Bruner suffered actual injury in the form of damages to and diminution in the value of her personal, health, and financial information – a form of intangible property that Plaintiff and Harrisburg entrusted to Defendant for the purpose of receiving accounting services from Defendant and which was compromised in, and as a result of, the Data Breach.

119. Plaintiff Bruner suffered imminent and impending injury arising from the substantially increased risk of future fraud, identity theft, and misuse posed by her Private Information being placed in the hands of criminals.

120. Plaintiff Bruner has a continuing interest in ensuring that her PII and PHI, which remain in the possession of Defendant, are protected and safeguarded from future breaches.

121. As a result of the Data Breach, Plaintiff Bruner made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach and reviewing financial accounts for any indications of actual or attempted identity theft or fraud. Plaintiff has spent several hours dealing with the Data Breach, valuable time she otherwise would have spent on other activities.

122. As a result of the Data Breach, Plaintiff Bruner has suffered anxiety as a result of the release of her PII and PHI, which she believed would be protected from unauthorized access and disclosure. These feelings include anxiety about unauthorized parties viewing, selling, and/or using her PII and PHI for purposes of committing cyber and other crimes against his including, but not limited to, fraud and identity theft. Plaintiff is very concerned about this increased,

substantial, and continuing risk, as well as the consequences that identity theft and fraud resulting from the Data Breach would have on her life.

123. Plaintiffs have suffered actual injury from having their Private Information compromised as a result of the Data Breach in the form of (a) damage to and diminution in the value of their PII and PHI, a form of property that Defendant obtained from Horizon Health, Harrisburg, and Plaintiffs; (b) violation of their privacy rights; and (c) present, imminent, and impending injury arising from the increased risk of identity theft, and fraud Plaintiffs now face.

124. As a result of the Data Breach, Plaintiffs anticipate spending considerable time and money on an ongoing basis to try to mitigate and address the many harms caused by the Data Breach.

125. In sum, Plaintiffs and Class Members have been damaged by the compromise of their Private Information in the Data Breach.

126. Plaintiffs and Class Members entrusted their Private Information to customers of Defendant in order to receive healthcare services.

127. Their Private Information was subsequently compromised as a direct and proximate result of the Data Breach, which Data Breach resulted from Defendant's inadequate data security practices.

128. As a direct and proximate result of KEB's actions and omissions, Plaintiffs and Class Members have been harmed and are at an imminent, immediate, and continuing increased risk of harm, including but not limited to, having medical services billed in their names, loans opened in their names, tax returns filed in their names, utility bills opened in their names, credit card accounts opened in their names, and other forms of identity theft.

129. Further, and as set forth above, as a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have also been forced to take the time and effort to mitigate the actual and potential impact of the data breach on their everyday lives, including placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

130. Plaintiffs and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

131. Plaintiffs and Class Members also face a substantial risk of being targeted in future phishing, data intrusion, and other illegal schemes through the misuse of their Private Information, since potential fraudsters will likely use such Private Information to carry out such targeted schemes against Plaintiffs and Class Members.

132. The Private Information maintained by and stolen from Defendant's systems, combined with publicly available information, allows nefarious actors to assemble a detailed mosaic of Plaintiffs and Class Members, which can also be used to carry out targeted fraudulent schemes against Plaintiff and Class Members.

133. Plaintiffs and Class Members also lost the benefit of the bargain they made with their healthcare providers and KEB. Plaintiffs and Class Members overpaid for services that were intended to be accompanied by adequate data security but were not. Thus, Plaintiffs and the Class did not receive the benefit of the bargain.

134. Additionally, Plaintiffs and Class Members also suffered a loss of value of their PII and PHI when it was acquired by cyber thieves in the Data Breach. Numerous courts have

recognized the propriety of loss of value damages in related cases. An active and robust legitimate marketplace for Private Information also exists. In 2019, the data brokering industry was worth roughly $200 billion.[25] In fact, consumers who agree to provide their web browsing history to the Nielsen Corporation can in turn receive up to $50 a year.[26]

135. As a result of the Data Breach, Plaintiffs' and Class Members' Private Information, which has an inherent market value in both legitimate and illegal markets, has been harmed and diminished due to its acquisition by cybercriminals. This transfer of valuable information happened with no consideration paid to Plaintiffs or Class Members for their property, resulting in an economic loss. Moreover, the Private Information is apparently readily available to others, and the rarity of the Private Information has been destroyed because it is no longer only held by Plaintiffs and the Class Members, and because that data no longer necessarily correlates only with activities undertaken by Plaintiffs and the Class Members, thereby causing additional loss of value.

136. Finally, Plaintiffs and Class Members have suffered or will suffer actual injury as a direct and proximate result of the Data Breach in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach.

137. Moreover, Plaintiffs and Class Members have an interest in ensuring that their Private Information, which is believed to still be in the possession of KEB, is protected from future breaches by the implementation of more adequate data security measures and safeguards, including but not limited to, ensuring that the storage of data or documents containing highly sensitive

[25] *See* https://thequantumrecord.com/blog/data-brokers-profit-from-our-data/#:~:text=The%20business%20of%20data%20brokering,annual%20revenue%20of%20%24200%20billion. (last visited on Aug. 20, 2024).

[26] *Frequently Asked Questions,* Nielsen Computer & Mobile Panel, https://computermobilepanel.nielsen.com/ui/US/en/faqen.html (last visited on Aug. 20, 2024).

personal and health information of its customers' patients is not accessible online, that access to such data is password-protected, and that such data is properly encrypted.

138. As a direct and proximate result of KEB's actions and inactions, Plaintiffs and Class Members have suffered a loss of privacy and have suffered cognizable harm, including an imminent and substantial future risk of harm, in the forms set forth above.

V. CLASS ACTION ALLEGATIONS

139. Plaintiffs bring this action individually and on behalf of all other persons similarly situated, pursuant to 735 ILCS 5/2-801.

140. Specifically, Plaintiffs propose the following Class, subject to amendment as appropriate:

> All citizens of the State of Illinois who had Private Information accessed and/or compromised as a result of the Data Breach discovered by KEB on or around February 7, 2023, including all persons who were sent a notice of the Data Breach.

141. Excluded from the Class are Defendant and its parents or subsidiaries, any entities in which it has a controlling interest, as well as its officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns. Also excluded is any Judge to whom this case is assigned as well as their judicial staff and immediate family members.

142. Plaintiffs reserves the right to modify or amend the definition of the proposed Class, as well as the add subclasses, before the Court determines whether certification is appropriate.

143. The proposed Class meets the criteria for certification under 735 ILCS 5/2-801/

144. Numerosity. The Class Members are so numerous that joinder of all members is impracticable. Though the exact number and identities of Class Members are unknown at this time, based on information and belief, the Class consists of thousands of patients of customers of KEB whose data was compromised in the Data Breach. The identities of Class Members are

ascertainable through KEB's records, Class Members' records, publication notice, self-identification, and other means.

145. 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 KEB engaged in the conduct alleged herein;

b. Whether KEB's conduct violated the FTCA and/or HIPAA;

c. When KEB learned of the Data Breach

d. Whether KEB's response to the Data Breach was adequate;

e. Whether KEB unlawfully lost or disclosed Plaintiffs' and Class Members' Private Information;

f. Whether KEB failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the Private Information compromised in the Data Breach;

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

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

i. Whether KEB owed a duty to Class Members to safeguard their Private Information;

j. Whether KEB breached its duty to Class Members to safeguard their Private Information;

k. Whether hackers obtained Class Members' Private Information via the Data Breach;

l. Whether KEB had a legal duty to provide timely and accurate notice of the Data Breach to Plaintiffs and the Class Members;

m. Whether KEB breached its duty to provide timely and accurate notice of the Data Breach to Plaintiffs and Class Members;

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

o. What damages Plaintiffs and Class Members suffered as a result of KEB's misconduct;

p. Whether KEB's conduct was negligent;

q. Whether KEB's conduct was *per se* negligent;

r. Whether KEB was unjustly enriched;

s. Whether Plaintiffs and Class Members are entitled to actual and/or statutory damages;

t. Whether Plaintiffs and Class Members are entitled to additional credit or identity monitoring and monetary relief; and

u. Whether Plaintiffs and Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

146. Typicality. Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' Private Information, like that of every other Class Member, was compromised in the Data Breach. Plaintiffs' claims are typical of those of the other Class Members because, *inter alia*,

all Class Members were injured through the common misconduct of KEB. Plaintiffs are advancing the same claims and legal theories on behalf of themselves and all other Class Members, and there are no defenses that are unique to Plaintiffs. The claims of Plaintiffs and those of Class Members arise from the same operative facts and are based on the same legal theories.

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

148. Predominance. KEB has engaged in a common course of conduct toward Plaintiffs and Class Members in that all of Plaintiffs' and Class Members' data was stored on the same computer systems and unlawfully accessed and exfiltrated in the same way. The common issues arising from KEB'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.

149. Superiority. A Class action is superior to other available methods 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. 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 KEB. In contrast, conducting 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.

150. Class certification is also appropriate because KEB has acted and/or refused to act on grounds generally applicable to the Class such that final injunctive relief and/or corresponding declaratory relief is appropriate as to the Class as a whole.

151. Finally, all members of the proposed Class are readily ascertainable. KEB has access to the names and addresses and/or email addresses of Class Members affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by KEB.

CLAIMS FOR RELIEF

COUNT I
NEGLIGENCE
(ON BEHALF OF PLAINTIFFS AND THE CLASS)

152. Plaintiffs restate and reallege all of the allegations stated above as if fully set forth herein.

153. KEB knowingly collected, came into possession of, and maintained Plaintiffs' and Class Members' Private Information, and had a duty to exercise reasonable care in safeguarding, securing, and protecting such Information from being disclosed, compromised, lost, stolen, and misused by unauthorized parties.

154. KEB's duty also included a responsibility to implement processes by which it could detect and analyze a breach of its security systems quickly and to give prompt notice to those affected in the case of a cyberattack.

155. KEB knew or should have known of the risks inherent in collecting the Private Information of Plaintiffs and Class Members and the importance of adequate security. KEB was

on notice because, on information and belief, it knew or should have known that it would be an attractive target for cyberattacks.

156. KEB owed a duty of care to Plaintiffs and Class Members whose Private Information was entrusted to it. KEB's duties included, but were not limited to, the following:

a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting Private Information in its possession;

b. To protect customers' patients' Private Information using reasonable and adequate security procedures and systems compliant with industry standards;

c. To have procedures in place to prevent the loss or unauthorized dissemination of Private Information in its possession;

d. To employ reasonable security measures and otherwise protect the Private Information of Plaintiffs and Class Members pursuant to HIPAA and the FTCA;

e. To implement processes to quickly detect a data breach and to timely act on warnings about data breaches; and

f. To promptly notify Plaintiffs and Class Members of the Data Breach, and to precisely disclose the type(s) of information compromised.

157. KEB's duty to employ reasonable data security measures arose, in part, 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.

158. KEB's duty also arose because Defendant was bound by industry standards to protect its customers' patients' confidential Private Information.

159. Plaintiffs and Class Members were foreseeable victims of any inadequate security practices on the part of Defendant, and KEB owed them a duty of care to not subject them to an unreasonable risk of harm.

160. KEB, through its actions and/or omissions, unlawfully breached its duty to Plaintiffs and Class Members by failing to exercise reasonable care in protecting and safeguarding Plaintiffs' and Class Members' Private Information within KEB's possession.

161. KEB, by its actions and/or omissions, breached its duty of care by failing to provide, or acting with reckless disregard for, fair, reasonable, or adequate computer systems and data security practices to safeguard the Private Information of Plaintiffs and Class Members.

162. KEB, by its actions and/or omissions, breached its duty of care by failing to promptly identify the Data Breach and then failing to provide prompt notice of the Data Breach to the persons whose Private Information was compromised.

163. KEB breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' Private Information. 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' Private Information;

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

c. Failing to periodically ensure that its email system maintained reasonable data security safeguards;

d. Allowing unauthorized access to Class Members' Private Information;

e. Failing to comply with the FTCA;

f. Failing to detect in a timely manner that Class Members' Private Information had been compromised; and

g. 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.

164. KEB acted with reckless disregard for the rights of Plaintiffs and Class Members by failing to provide prompt and adequate individual notice of the Data Breach such that Plaintiffs and Class Members could take measures to protect themselves from damages caused by the fraudulent use of the Private Information compromised in the Data Breach.

165. KEB had a special relationship with Plaintiffs and Class Members. Healthcare providers willingness to entrust KEB with their Private Information was predicated on the understanding that KEB would take adequate security precautions. Moreover, only KEB had the ability to protect its systems (and the Private Information that it stored on them) from attack.

166. KEB's breach of duties owed to Plaintiffs and Class Members caused Plaintiffs' and Class Members' Private Information to be compromised and exfiltrated as alleged herein.

167. KEB's breaches of duty also caused a substantial, imminent risk to Plaintiffs and Class Members of identity theft, loss of control over their Private Information, and/or loss of time and money to monitor their accounts for fraud.

168. As a result of KEB's negligence in breach of its duties owed to Plaintiffs and Class Members, Plaintiffs and Class Members are in danger of imminent harm in that their Private Information, which is still in the possession of third parties, will be used for fraudulent purposes.

169. KEB also had independent duties under state laws that required it to reasonably safeguard Plaintiffs' and Class Members' Private Information and promptly notify them about the Data Breach.

170. As a direct and proximate result of KEB's negligent conduct, Plaintiffs and Class Members have suffered damages as alleged herein and are at imminent risk of further harm.

171. The injury and harm that Plaintiffs and Class Members suffered was reasonably foreseeable.

172. Plaintiffs and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

173. In addition to monetary relief, Plaintiffs and Class Members are also entitled to injunctive relief requiring KEB to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members.

COUNT II
NEGLIGENCE *PER SE*
(ON BEHALF OF PLAINTIFFS AND THE CLASS)

174. Plaintiffs restate and reallege the allegations in the preceding paragraphs as if fully set forth herein.

175. Pursuant to Section 5 of the FTCA, KEB had a duty to provide fair and adequate computer systems and data security to safeguard the Private Information of Plaintiffs and Class Members.

176. Pursuant to HIPAA, 42 U.S.C. § 1302(d), *et seq*., KEB had a duty to implement reasonable safeguards to protect Plaintiffs' and Class Members' Private Information.

177. Specifically, pursuant to HIPAA, Defendant had a duty to render the electronic PHI it maintained unusable, unreadable, or indecipherable to unauthorized individuals by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning

meaning without the use of a confidential process or key." *See* definition of "encryption" at 45 C.F.R. § 164.304.

178. KEB breached its duties to Plaintiffs and Class Members under the FTCA and HIPAA by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information.

179. Specifically, KEB breached its duties by failing to employ industry-standard cybersecurity measures in order to comply with the FTCA, including but not limited to proper segregation, access controls, password protection, encryption, intrusion detection, secure destruction of unnecessary data, and penetration testing.

180. The FTCA prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice of failing to use reasonable measures to protect PII and PHI (such as the Private Information compromised in the Data Breach). The FTC rulings and publications described above, together with the industry-standard cybersecurity measures set forth herein, form part of the basis of KEB's duty in this regard.

181. KEB also violated the FTCA and HIPAA by failing to use reasonable measures to protect the Private Information of Plaintiffs and the Class and by not complying with applicable industry standards, as described herein.

182. It was reasonably foreseeable, particularly given the growing number of data breaches of Private Information, that the failure to reasonably protect and secure Plaintiffs' and Class Members' Private Information in compliance with applicable laws would result in an unauthorized third-party gaining access to KEB's networks, databases, and computers that stored Plaintiffs' and Class Members' unencrypted Private Information.

183. Plaintiffs and Class Members are within the class of persons that the FTCA and HIPAA are intended to protect and KEB's failure to comply with both constitutes negligence *per se*.

184. Plaintiffs' and Class Members' Private Information constitutes personal property that was stolen due to KEB's negligence, resulting in harm, injury, and damages to Plaintiffs and Class Members.

185. As a direct and proximate result of KEB's negligence *per se*, Plaintiffs and the Class have suffered, and continue to suffer, injuries and damages arising from the unauthorized access of their Private Information, including but not limited to damages from the lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives.

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

187. In addition to monetary relief, Plaintiffs and Class Members are also entitled to injunctive relief requiring KEB to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members.

COUNT III
UNJUST ENRICHMENT
(ON BEHALF OF PLAINTIFFS AND THE CLASS)

188. Plaintiffs restate and reallege the allegations in the preceding paragraphs as if fully set forth herein.

189. Plaintiffs and Class Members conferred a benefit on KEB by turning over their Private Information to Defendant's customers and by paying for service that should have included

cybersecurity protection to protect their Private Information. Plaintiffs and Class Members did not receive such protection.

190. Upon information and belief, KEB funds its data security measures entirely from its general revenue, including from payments made to it by Plaintiffs' and Class Members' healthcare providers.

191. As such, a portion of the payments made by Plaintiffs' and Class Members' healthcare providers is to be used to provide a reasonable and adequate level of data security that is in compliance with applicable state and federal regulations and industry standards, and the amount of the portion of each payment made that is allocated to data security is known to KEB.

192. KEB has retained the benefits of its unlawful conduct, including the amounts of payment received from Plaintiffs' and Class Members' healthcare providers that should have been used for adequate cybersecurity practices that it failed to provide.

193. KEB knew that Plaintiffs' and Class Members' healthcare providers conferred a benefit upon it, which KEB accepted. KEB profited from these transactions and used the Private Information of Plaintiffs and Class Members for business purposes, while failing to use the payments it received for adequate data security measures that would have secured Plaintiffs' and Class Members' Private Information and prevented the Data Breach.

194. If Plaintiffs and Class Members healthcare providers had known that KEB had not adequately secured their Private Information, they would not have agreed to provide such Private Information to Defendant.

195. Due to KEB's conduct alleged herein, it would be unjust and inequitable under the circumstances for KEB to be permitted to retain the benefit of its wrongful conduct.

196. As a direct and proximate result of KEB's conduct, Plaintiffs and Class Members have suffered, and/or are at a continued, imminent risk of suffering, injury that includes but is not limited to the following: (i) actual identity theft; (ii) the loss of the opportunity to control how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their Private Information, which remains in KEB's possession and is subject to further unauthorized disclosures so long as KEB fails to undertake appropriate and adequate measures to protect Private Information in its continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

197. Plaintiffs and Class Members are entitled to full refunds, restitution, and/or damages from KEB and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by KEB from its wrongful conduct. This can be accomplished by establishing a constructive trust from which the Plaintiffs and Class Members may seek restitution or compensation.

198. Plaintiffs and Class Members may not have an adequate remedy at law against KEB, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

COUNT IV
BREACH OF FIDUCIARY DUTY
(ON BEHALF OF PLAINTIFFS AND THE CLASS)

199. Plaintiffs restate and reallege the allegations in the preceding paragraphs as if fully set forth herein.

200. In light of the special relationship between KEB and its customers' patients, whereby KEB became a guardian of Plaintiffs' and Class Members' Private Information (including highly sensitive, confidential, personal, and other PHI) KEB was a fiduciary, created by its undertaking and guardianship of the Private Information, to act primarily for the benefit of its customers' patients, including Plaintiffs and Class Members. This benefit included (1) the safeguarding of Plaintiffs' and Class Members' Private Information; (2) timely notifying Plaintiffs and Class Members of the Data Breach; and (3) maintaining complete and accurate records of what and where KEB's customers' patients' Private Information was and is stored.

201. KEB had a fiduciary duty to act for the benefit of Plaintiffs and the Class upon matters within the scope of its customers' patients' relationship, in particular to keep the Private Information secure.

202. KEB breached its fiduciary duties to Plaintiffs and Class Members by failing to diligently investigate the Data Breach to determine the number of Class Members affected and notify them within a reasonable and practicable period of time.

203. KEB breached its fiduciary duties to Plaintiffs and the Class by failing to protect their Private Information.

204. KEB breached its fiduciary duties to Plaintiffs and Class Members by failing to ensure the confidentiality and integrity of electronic PHI KEB created, received, maintained, and transmitted, in violation of 45 CFR 164.306(a)(1).

205. KEB breached its fiduciary duties to Plaintiffs and Class Members by failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights, in violation of 45 CFR 164.312(a)(1).

206. KEB breached its fiduciary duties to Plaintiffs and Class Members by failing to implement policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 CFR 164.308(a)(1).

207. KEB breached its fiduciary duties to Plaintiffs and Class Members by 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 CFR 164.308(a)(6)(ii).

208. KEB breached its fiduciary duties to Plaintiffs and Class Members by failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic PHI, in violation of 45 CFR 164.306(a)(2).

209. KEB breached its fiduciary duties to Plaintiffs and Class Members by failing to protect against any reasonably-anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 CFR 164.306(a)(3).

210. KEB breached its fiduciary duties to Plaintiffs and Class Members by failing to ensure compliance with the HIPAA security standard rules by its workforce, in violation of 45 CFR 164.306(a)(94).

211. KEB breached its fiduciary duties to Plaintiffs and Class Members by impermissibly and improperly using and disclosing PHI that is and remains accessible to unauthorized persons, in violation of 45 CFR 164.502, *et seq.*

212. As a direct and proximate result of KEB's breaches of its fiduciary duties, Plaintiffs and Class Members have suffered and will continue to suffer the harms and injuries alleged herein, as well as anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

COUNT V
BREACH OF THIRD-PARTY BENEFICIARY CONTRACT
(ON BEHALF OF PLAINTIFFS AND THE CLASS)

213. Plaintiffs restate and reallege the allegations in the preceding paragraphs as if fully set forth herein.

214. Defendant entered into contracts, written or implied, with its clients to perform services that include, but are not limited to, providing accounting services for healthcare providers. Upon information and belief, these contracts are virtually identical between and among Defendant and its clients around the country whose patients, including Plaintiffs and Class Members, were affected by the Data Breach.

215. In exchange, Defendant agreed, in part, to implement adequate security measures to safeguard the PII and PHI of Plaintiffs and the Class.

216. These contracts were made expressly for the benefit of Plaintiffs and the Class, as Plaintiffs and Class Members were the intended third-party beneficiaries of the contracts entered into between Defendant and its clients. Defendant knew that if it were to breach these contracts with its clients, the clients' patients—Plaintiffs and Class Members—would be harmed.

217. Defendant breached the contracts it entered into with its clients by, among other things, failing to (i) use reasonable data security measures, (ii) implement adequate protocols and employee training sufficient to protect Plaintiffs' Private Information from unauthorized disclosure to third parties, and (iii) promptly and adequately detecting the Data Breach and notifying Plaintiffs and Class Members thereof.

218. Plaintiffs and the Class were harmed by Defendant's breach of its contracts with its clients, as such breach is alleged herein, and are entitled to the losses and damages they have sustained as a direct and proximate result thereof.

219. Plaintiffs and Class Members are also entitled to their costs and attorney's fees incurred in this action.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and the Class described above, seeks the following relief:

a. An order certifying this action as a Class action under 735 ILCS 5/2-801, defining the Class as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiffs are a proper representatives of the Class requested herein;
b. Judgment in favor of Plaintiffs and Class Members awarding them appropriate monetary relief, including actual damages, statutory damages, equitable relief, restitution, disgorgement, and statutory costs;
c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class as requested herein;
d. An order instructing KEB to purchase or provide funds for lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members;

e. An order requiring KEB to pay the costs involved in notifying Class Members about the judgment and administering the claims process;

f. A judgment in favor of Plaintiff and Class Members awarding them prejudgment and post-judgment interest, reasonable attorneys' fees, costs, and expenses as allowable by law; and

g. An award of such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury on all triable issues.

Dated: April 11, 2025

Respectfully submitted,

By: */s/ Cassandra P. Miller*
Cassandra P. Miller
STRAUSS BORRELLI PLLC
980 N Michigan Ave, Suite 1610
Chicago, IL 60611
Telephone: (872) 263-1100
Facsimile: (872) 263-1109
cmiller@straussborrelli.com

Tyler J. Bean (*Pro Hac Vice* forthcoming)
SIRI & GLIMSTAD LLP
745 Fifth Avenue, Suite 500
New York, New York 10151
Telephone: (212) 532-1091
tbean@sirillp.com

Gary Klinger
MILBERG COLEMAN PHILLIPS GROSSMAN, PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Telephone: (866) 252-0878
gklinger@milberg.com

— EXHIBIT A —

keb
P.O. Box 989728
West Sacramento, CA 95798-9728

[redacted]

August 12, 2024

NOTICE OF SECURITY INCIDENT

Dear Tracey Bruner:

Kerber, Eck & Braeckel LLP ("KEB") is an accounting and tax services firm that provides services to a client organization with which you are affiliated. On behalf of its client, Crawford Hospital District D.b.a. Crawford Memorial Hospital, KEB's Marion, Illinois branch is writing to inform you of an incident that may impact the privacy of some of your information. We are providing you with this notice, which provides details about the incident, our response to it, and the resources available to assist you in safeguarding your information, should you feel it is appropriate to do so.

Who is KEB / Why Do You Have My Information? KEB provides services to Crawford Hospital District D.b.a Crawford Memorial Hospital, and we understand you to be associated with this organization. As part of those services KEB handles information relating to individuals. This cybersecurity incident occurred with KEB and did not impact th computer systems of Crawford Hospital District D.b.a. Crawford Memorial Hospital.

What Happened? On February 7, 2023, KEB's Marion, Illinois branch became aware of suspicious activity on o computer network. We immediately launched an investigation to determine the nature and scope of the issue. T investigation determined that an unauthorized actor accessed our network between January 27 and February 7, 202 and viewed or copied certain files stored on our network. As a result, KEB quickly began working with a third-party perform a thorough and time-intensive review of the potentially impacted files determine the types of informati contained in the account and to whom the information belonged. This review determined that impacted files contain certain information related to you. KEB then notified Crawford Hospital District D.b.a. Crawford Memorial Hosp regarding this incident and worked with them to obtain good address information for you, if that was not available KEB. On July 9, 2024, the address enrichment process completed, and KEB began providing notice to you.

What Information Was Involved? Our review determined the following information related to you was present wi the impacted files: date of birth, medical record number, and treatment information and name. At this time, we hav evidence of identity theft or fraud in relation to this incident.

What We Are Doing. The security of information in our care is a top priority for KEB. We quickly responded to incident by securing our network and determining what sensitive information may have been impacted. As part o ongoing commitment to the privacy and security of information in our care, we have implemented an advanced t detection and response tool throughout our network and are reviewing existing policies and procedures related to security. We also reported this event to federal law enforcement and appropriate privacy regulators where required.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by revi your account statements and ss reports for suspicious activity. You can find out more about how to better p against the potential misuse of information in the enclosed *Steps You Can Take to Protect Personal Information*.