UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

ROBERT BLACKWELL, on behalf of himself and all others similarly situated, Plaintiff, v. KRAEMER NORTH AMERICA, LLC, Defendant.	Case No. 0:23-cv-1851 **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

CONSOLIDATED CLASS ACTION COMPLAINT

Plaintiff Robert Blackwell ("Plaintiff"), individually and on behalf of all others similarly situated, by and through his attorneys, brings this class action against Kraemer North America, LLC, ("Kraemer" or "Defendant"), upon personal knowledge as to himself and his own acts and experiences, and upon information and belief as to all other matters, including his counsel's investigation, allege as follows. Plaintiff believes that additional evidentiary support exists for his allegations, given an opportunity for discovery.

INTRODUCTION AND NATURE OF ACTION

1. Kraemer is a national heavy civil contractor that focuses on transportation, rail, and marine construction related projects. Kraemer is based in Wisconsin with a significant presence via regional offices in Minnesota, Colorado, Washington, and Utah.

2. As such, Defendant stores a litany of highly sensitive personal identifiable information ("PII") about its current and former employees. But Defendant lost control over that data when cybercriminals infiltrated its insufficiently protected computer systems in a data breach (the "Data Breach").

3. Thus, Defendant had no effective means to prevent, detect, stop, or mitigate breaches of its systems—thereby allowing cybercriminals unrestricted access to employee PII.

4. On information and belief, cybercriminals were able to breach Defendant's systems because Defendant failed to adequately train its employees on cybersecurity and failed to maintain reasonable security safeguards or protocols to protect the Class's PII. In short, Defendant's failures placed the Class's PII in a vulnerable position—rendering them easy targets for cybercriminals.

5. Plaintiff is a Data Breach victim, receiving breach notice in April 2023. He brings this class action on behalf of himself and all others harmed by Defendant's misconduct.

6. Plaintiff brings this class action against Kraemer for its failure to secure and safeguard the confidential, personally identifiable information of its employees. The categories of stolen information about Kraemer's current and former employees included names, addresses, Social Security numbers, driver's license number or other government identification, and bank account numbers (the "PII").

7. Due to Defendant's negligence, Plaintiff and the Class have suffered harm and are subject to a present and continuing risk of identity theft. Plaintiff's and the Class's PII has been compromised and they must now undertake additional security measures to mitigate the damage caused by Defendant.

8. Plaintiff Blackwell is a former Kraemer employee and Data Breach victim. Mr. Blackwell worked for Kraemer in 2022 and 2023, and, as a condition of that employment, was required to provide his PII to Kraemer. Plaintiff reasonably believed that Defendant would take adequate steps to safeguard the PII he entrusted to it. Defendant did not, resulting in the Data Breach.

9. The Data Breach impacted many of Kraemer's current and former employees. The full scope of the Data Breach, however, is either not known or has not been publicly disclosed.

10. Plaintiff brings this Complaint on behalf of persons whose PII was stolen during the Data Breach.

PARTIES

11. Plaintiff Robert Blackwell is a resident of Duluth, Minnesota. Mr. Blackwell received a notice from Defendant in April 2023 that his PII was exposed during Kraemer's Data Breach.

12. Kraemer North America, LLC is a limited liability company construction contractor incorporated in Delaware and headquartered in Wisconsin, with its principal place of business located at One Plainview Road, Plain, Wisconsin. It maintains a regional office in Burnsville, MN that is responsible for its operations in the Upper Midwest Region.

JURISDICTION AND VENUE

13. This Court has 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, and there are more than 100 putative class members. Plaintiff and Kraemer are citizens of different states. Class members and Kraemer are also of different states.

14. This Court has jurisdiction over Kraemer because it regularly conducts business in Minnesota and has sufficient minimum contacts in Minnesota. Kraemer has intentionally availed itself of this jurisdiction by locating a regional office in Minnesota.

15. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because Plaintiff is a resident in this District and Kraemer's conducts regular business in this District.

FACTUAL BACKGROUND

Kraemer North America, LLC

16. Kraemer is a construction company established in 1911, located in Plain, Wisconsin, who claims to have "a national reputation for quality and safety" and is a full service heavy civil contractor serving the transportation, rail, and marine markets.[1]

17. Kraemer employs numerous construction professionals. Plaintiff is a former employee of Kraemer.

18. As detailed more fully below, Kraemer failed to safely and securely store the PII entrusted to it by its current and former employees and failed to prevent it from being compromised during the Data Breach.

Kraemer Collected and Stored the PII of Plaintiff and the Class

19. As part of its business, Defendant receives and maintains the PII of thousands of current and former employees. In doing so, Defendant implicitly promises to safeguard their PII.

20. In collecting and maintaining the PII, Defendant agreed it would safeguard the data in accordance with its internal policies, state law, and federal law. After all, Plaintiff and Class Members themselves took reasonable steps to secure their PII.

21. Under state and federal law, businesses like Defendant have duties to protect employees' PII and to notify them about breaches.

The Data Breach

22. On March 19, 2023, Defendant identified unusual activity in its network. It was subsequently discovered that Defendant's network was hacked in a Data Breach. That Data Breach

[1] KRAMER NORTH AMERICA, https://kraemerna.com/, last accessed (June 16, 2023).

then lasted for six days or more—giving criminals plenty of time to seize Plaintiff's and the Class's exposed PII.[2] Moreover, Defendant did not even provide victims with notice of the Data Breach until at least April 2023—more than a month after the start of the breach.[3]

23. Simply put, Defendant failed in its duties when its inadequate security practices caused the Data Breach.

24. Thus, Defendant kept the Class in the dark—thereby depriving the Class of the opportunity to try and mitigate their injuries in a timely manner.

25. And when it did notify Plaintiff and the Class of the Data Breach, Defendant acknowledged that the Data Breach puts them at a present, continuing, and significant risk of suffering identity theft, warning them to "be vigilant for incidents of fraud or identity theft by reviewing your account statements and monitoring free credit reports for any unauthorized activity."[4]

26. Since the breach, Defendant has not informed the Plaintiff or the Class of any additional security related measures it is taking to try and secure the PII it has already lost control of once.

27. On information and belief, Defendant failed to adequately train its employees on reasonable cybersecurity protocols or implement reasonable security measures.

28. Defendant's negligence is further evidenced by its failure to prevent the Data Breach and stop cybercriminals from accessing the PII.

29. Defendant has done little to remedy its Data Breach. True, Defendant has offered concessions of credit monitoring and identity services to Plaintiff and the Class.[5] But upon

[2] Data Breach Notice, attached as **Exhibit A.**
[3] *Id.*
[4] *Id.*
[5] *Id.*

information and belief, such services do not properly compensate Plaintiff and Class Members for the injuries that Defendant inflicted upon them.

30. Because of Defendant's Data Breach, the sensitive PII of the Plaintiff and Class Members were placed into the hands of cybercriminals—inflicting numerous injuries and significant damages upon Plaintiff and Class Members.

Data Breaches Lead to Identity Theft and Cognizable Injuries.

31. The personal and financial information of Plaintiff and the Class is valuable and has been commoditized in recent years.

32. It can take victims years to discover such identity theft and fraud. This gives criminals plenty of time to sell the PII far and wide.

33. The ramifications of Defendant's failure to keep Plaintiff's and the Class's PII secure are severe. Identity theft occurs when someone uses another's personal and financial information such as that person's name, account number, Social Security number, driver's license number, date of birth, and/or other information, without permission, to commit fraud or other crimes.

34. According to experts, one out of four data breach notification recipients become a victim of identity fraud.[6]

35. Stolen PII is often trafficked on the "dark web," a heavily encrypted part of the Internet that is not accessible via traditional search engines. Law enforcement has difficulty policing the "dark web" due to this encryption, which allows users and criminals to conceal identities and online activity.

[6] Study Shows One in Four Who Receive Data Breach Letter Become Fraud Victims, ThreatPost.com (last visited, Feb. 21, 2013), https://threatpost.com/study-shows-one-four-who-receive-data-breach-letter-become-fraud-victims-022013/77549/

36. Once PII is sold, it is often used to gain access to various areas of the victim's digital life, including bank accounts, social media, credit card, and tax details. This can lead to additional PII being harvested from the victim, as well as PII from family, friends, and colleagues of the original victim.

37. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses that year, resulting in more than $3.5 billion in losses to individuals and business victims.

38. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good." Kraemer did not rapidly report to Plaintiff and the Class that their PII had been stolen.

39. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

40. Data breaches facilitate identity theft as hackers obtain victim's PII and use it to siphon money from existing accounts, open new accounts in the names of their victims, or sell victims' PII to others who do the same.

41. Victims of identity theft often suffer indirect financial costs as well, including the costs incurred due to litigation initiated by creditors and in overcoming the many obstacles they face in obtaining or retaining credit.

42. In addition to out-of-pocket expenses that can exceed thousands of dollars for the victim of new account identity theft, and the emotional toll identity theft can take, some victims have to spend a considerable time repairing the damage caused by the theft of their PII. Victims of new account identity theft will likely have to spend time correcting fraudulent information in their

credit reports and continuously monitor their reports for future inaccuracies, close existing bank/credit accounts, open new ones, and dispute charges with creditors.

43. Further complicating the issues faced by victims of identity theft, data thieves may wait years before attempting to use the stolen PII. To protect themselves, Plaintiff and the Class will need to remain vigilant against unauthorized data use for years or even decades to come.

44. The Federal Trade Commission ("FTC") has also recognized that consumer data is a new (and valuable) form of currency. In a FTC roundtable presentation, former Commissioner, Pamela Jones Harbour, underscored this point by reiterating that "most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency."[7]

45. Stolen PII is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII can be worth up to $1,000.00 depending on the type of information obtained.[8]

46. The FTC has also issued numerous guidelines for businesses that highlight the importance of reasonable data security practices. The FTC has noted the need to factor data security into all business decision-making.[9] According to the FTC, data security requires: (1) encrypting information stored on computer networks; (2) retaining payment card information only as long as necessary; (3) properly disposing of personal information that is no longer needed; (4) limiting administrative access to business systems; (5) using industry unapproved activity; (6)

[7] Statement of FTC Commissioner Pamela Jones Harbour—Remarks Before FTC Exploring Privacy Roundtable, (Dec. 7, 2009), http://www.ftc.gov/speeches/harbour/091207privacyroundtable.pdf (last visited September 22, 2021).
[8] *See* Here's How Much Your Personal Information Is Selling for on the Dark Web, Experian, https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited February 12, 2023).

[9] Start With Security, A Guide for Business, FTC, https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf

monitoring activity on networks to uncover unapproved activity; (7) verifying that privacy and security features function properly; (8) testing for common vulnerabilities; and (9) updating and patching third-party software.[10]

47. According to the FTC, unauthorized PII disclosures wreak havoc on consumers' finances, credit history and reputation, and can take time, money and patience to resolve the fallout.[11] The FTC, as such, treats 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(a) of the FTC Act.

48. To that end, the FTC has issued orders against businesses that failed to employ reasonable measures to secure sensitive payment card data. *See In the matter of Lookout Services, Inc.*, No. C-4326, ⁋ 7 (June 15, 2011) ("[Kraemer] allowed users to bypass authentication procedures" and "failed to employ sufficient measures to detect and prevent unauthorized access to computer networks, such as employing an intrusion detection system and monitoring system logs."); *In the matter of DSW, Inc.*, No. C-4157, ⁋ 7 (Mar. 7, 2006) ("[Kraemer] failed to employ sufficient measures to detect unauthorized access."); *In the matter of The TJX Cos., Inc.*, No. C-4227 (Jul. 29, 2008) ("[R]espondent stored . . . personal information obtained to verify checks and process unreceipted returns in clear text on its in-store and corporate networks[,]" "did not require network administrators . . . to use different passwords to access different programs, computers, and networks[,]" and "failed to employ sufficient measures to detect and prevent unauthorized access to computer networks . . ."); *In the matter of Dave & Buster's Inc.*, No. C-4291 (May 20, 2010) ("[Kraemer] failed to monitor and filter outbound traffic from its networks to identify and

[10] *Id*.
[11] See Taking Charge, What to Do If Your Identity is Stolen, FTC, at 3 (2012), www.consumer.ftc.gov/articles/pdf-0009-taking-charge.pdf.

block export of sensitive personal information without authorization" and "failed to use readily available security measures to limit access between instore networks . . ."). These orders, which all preceded Kraemer's Data Breach, further clarify the measures businesses must take to meet their data security obligations.

49. Consumers place a high value on their PII and a greater value on their PHI, in addition to the privacy of their PII. Research shows how much consumers value their data privacy, and the amount is considerable. Indeed, studies confirm that "[a]mong U.S. subjects, protection against errors, improper access, and secondary use of personal information is worth US $30.49–44.62."[12]

50. By virtue of the Data Breach here and unauthorized release and disclosure of the PII of Plaintiff and the Class, Kraemer deprived Plaintiff and the Class of the substantial value of their PII, to which they are entitled. As previously alleged, Kraemer failed to provide reasonable and adequate data security, pursuant to and in compliance with industry standards and applicable law.

51. Identity theft associated with data breaches is particularly pernicious due to the fact that the information is made available, and has usefulness to identity thieves, for an extended period of time after it is stolen.

52. As a result, victims suffer immediate and long-lasting exposure and are susceptible to further injury over the passage of time.

53. Even absent any adverse use, consumers suffer injury from the simple fact that information associated with their financial accounts and identity has been stolen. When PII is

[12] See Il-Horn Hann et al., The Value of Online Information Privacy (Oct. 2002) available at http://www.comp.nus.edu.sg/~ipng/research/privacy.pdf (last visited September 22, 2021); see also Tsai, Cranor, Acquisti, and Egelman, The Effect of Online Privacy Information on Purchasing Behavior, 22 (2) Information Systems Research 254, 254 (June 2011).

stolen, accounts become less secure, and the information once used to sign up for bank accounts and other financial services is no longer as reliable as it had been before the theft. Thus, consumers must spend time and money to re-secure their financial position and rebuild the good standing they once had in the financial community.

54. As a direct and proximate result of Kraemer's wrongful actions and omissions here, Plaintiff and the Class have suffered, and will continue to suffer, ascertainable losses, economic damages, and other actual injury and harm, including, *inter alia*: (i) from the untimely and inadequate notification of the Data Breach, (ii) the resulting immediate and continuing risk of future ascertainable losses, economic damages and other actual injury and harm, (iii) the opportunity cost and value of lost time they must spend to monitor their financial accounts and other accounts—for which they are entitled to compensation; (iv) out-of-pocket expenses for securing identity theft protection and other similar necessary services; (v) the diminution in value of their PII; (vi) the compromise and continuing publication of their PII; (vii) unauthorized use of stolen PII; and (viii) 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 the appropriate measures to protect the PII in their possession.

Defendant Failed to Adhere to FTC Guidelines

55. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making. To that end, the FTC has issued numerous guidelines identifying best data security practices that businesses, such as Defendant, should employ to protect against the unlawful exposure of PII.

56. 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. The guidelines explain that businesses should:

a. protect the personal customer information that they keep;

b. properly dispose of personal information that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

57. 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.

58. The FTC recommends that companies not maintain information 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.

59. 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.

60. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to employees' PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

Plaintiff's Experiences and Injuries

61. Plaintiff was injured by Defendant's Data Breach.

62. Plaintiff was employed by Defendant, but his employment ended in January 2023.

63. As a condition of his employment with Defendant, Plaintiff provided Defendant with his PII. Defendant used that PII to facilitate its employment of Plaintiff, including payroll, and required Plaintiff to provide that PII to obtain employment and payment for that employment.

64. Plaintiff provided his PII to Defendant and trusted the company would use reasonable measures to protect it according to Defendant's internal policies, as well as state and federal law. Defendant obtained and continues to maintain Plaintiff's PII and has a continuing legal duty and obligation to protect that PII from unauthorized access and disclosure.

65. Through its Data Breach, Defendant compromised Plaintiff's PII. To which, Plaintiff received a Notice of Data Breach dated April 2023.

66. Since the Data Breach, Plaintiff has been the victim of identity theft. Someone attempted to open credit cards in Plaintiff's name and Plaintiff received numerous emails and letters stating he was being denied credit cards, that Plaintiff did not attempt to open. Additionally, Plaintiff's credit score decreased from 620 to 380.

67. Plaintiff has also suffered from an increasing flood of spam texts and phone calls.

68. Plaintiff has spent—and will continue to spend—significant time and effort monitoring his accounts to protect himself from identity theft, and, in fact, Defendant directed him

to take those steps in its breach notice. Plaintiff fears for his personal financial security and worries about what information was exposed in the Data Breach, specifically his Social Security number.

69. Because of Defendant's Data Breach, Plaintiff has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, Plaintiff's injuries are precisely the type of injuries that the law contemplates and addresses.

70. Plaintiff suffered actual injury from the exposure (and likely theft) of his PII—which violates his rights to privacy.

71. Plaintiff suffered actual injury in the form of damages to and diminution in the value of his PII. After all, PII is a form of intangible property—property that Defendant was required to adequately protect.

72. Plaintiff suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because Defendant's Data Breach placed Plaintiff's PII right in the hands of criminals.

73. Because of the Data Breach, Plaintiff anticipates spending considerable amounts of time and money to try and mitigate his injuries.

74. Today, Plaintiff has a continuing interest in ensuring that his PII—which, upon information and belief, remains backed up in Defendant's possession—is protected and safeguarded from additional breaches.

CLASS DEFINITION AND ALLEGATIONS

75. Plaintiff brings this class action pursuant to Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3), individually and on behalf of all members of the following class:

> All individuals residing in the United States whose PII was compromised in the Data Breach disclosed by Kraemer in April 2023, including all those who received notice of the breach.

76. Excluded from the Class are Kraemer, their agents, affiliates, parents, subsidiaries, any entity in which Kraemer has a controlling interest, any Kraemer officer or director, any successor or assign, and any Judge who adjudicates this case, including their staff and immediate family.

77. Plaintiff reserves the right to amend the class definition.

78. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of his claims on class-wide bases using the same evidence as would be used to prove those elements in individual actions asserting the same claims.

a. **Numerosity**. The members of the Class are so numerous that joinder of all members of the Class is impracticable.

b. **Commonality and Predominance**. Plaintiff and the Class's claims raise predominantly common fact and legal questions, which predominate over any questions affecting individual Class members, that a class wide proceeding can answer for all Class members. Indeed, it will be necessary to answer the following questions:

i. Whether Kraemer had a duty to use reasonable care in safeguarding Plaintiff and the Class's PII;

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

iii. Whether Kraemer was negligent in maintaining, protecting, and securing Plaintiff and the Class's PII;

iv. Whether Kraemer breached contract promises to safeguard Plaintiff and the Class's PII;

v. Whether Kraemer took reasonable measures to determine the extent of the Data Breach after discovering it;

vi. Whether Kraemer's Breach Notice was reasonable;

vii. Whether the Data Breach caused Plaintiff and the Class's injuries;

viii. What the proper damages measure is; and

ix. Whether Plaintiff and the Class are entitled to damages, treble damages, or injunctive relief.

c. **Typicality**. Plaintiff's claims are typical of Class member's claims as each arises from the same Data Breach, the same alleged violations by Kraemer, and the same unreasonable manner of notifying individuals about the Data Breach.

d. **Adequacy**. Plaintiff will fairly and adequately protect the proposed Class's common interests. His interests do not conflict with Class members' interests. He has also retained counsel experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf, including as lead counsel.

e. **Superiority.** A class action is superior to all other available means for the fair and efficient adjudication of this controversy. The damages or other financial detriment suffered by individual Class members are relatively small compared to the burden and expense that would be entailed by individual litigation of their claims against Defendant. It would thus be virtually impossible for the Class members, on an individual basis, to obtain effective redress for the wrongs done to them. Individualized litigation would create the danger of inconsistent or contradictory judgments arising

from the same set of facts and would also increase the delay and expense to all parties and the courts. By contrast, the class action device provides the benefits of adjudication of these issues in a single proceeding, ensures economies of scale and comprehensive supervision by a single court, and presents no unusual management difficulties under the circumstances here.

FIRST CAUSE OF ACTION
Negligence
(On Behalf of Plaintiff and the Class)

79. Plaintiff incorporates by reference all previous allegations as though fully set forth herein.

80. Kraemer owed to Plaintiff and the Class a duty of reasonable care to protect Plaintiff's and the Class's data from the foreseeable threat of theft during a Data Breach. This duty arose from several sources.

81. Plaintiff and members of the Class entrusted their PII to Kraemer. Defendant owed a duty to Plaintiff and the Class to exercise reasonable care in safeguarding and protecting their personal data and keeping it from being compromised, lost, stolen, misused, and or/disclosed to unauthorized parties. This duty included, among other things, designing, maintaining, and testing Defendant's security systems to ensure the personal data of Plaintiff's and the Class was adequately secured and protected, including using encryption technologies. Defendant further had a duty to implement processes that would detect a breach of its security system in a timely manner.

82. Kraemer was under a basic duty to act with reasonable care when it undertook to collect, create, and store Plaintiff's and the Class's sensitive data on its computer system, fully aware–as any reasonable entity of its size would be–of the prevalence of data breaches and the

resulting harm such a breach would cause. The recognition of Defendant's duty to act reasonably in this context is consistent with, *inter alia*, the Restatement (Second) of Torts § 302B (1965), which recounts a basic principle: an act or omission may be negligent if the actor realizes or should realize it involves an unreasonable risk of harm to another, even if the harm occurs through the criminal acts of a third party.

83. Kraemer also owed a duty to timely and accurately disclose the scope, nature, and occurrence of the Data Breach. This disclosure is necessary so Plaintiff and the Class can take appropriate measures to avoid unauthorized use of their PII, accounts, cancel and/or change usernames and passwords on compromised accounts, monitor their accounts to prevent fraudulent activity, contact their financial institutions about compromise or possible compromise, obtain credit monitoring services, and/or take other steps in an effort to mitigate the harm caused by the Data Breach and Kraemer's unreasonable misconduct.

84. Defendant knew that the personal data of Plaintiff and the Class was personal and PII that is valuable to identity thieves and other criminals. Defendant also knew of the serious harms that could happen if the personal data of Plaintiff and the Class was wrongfully disclosed, that disclosure was not fixed.

85. By being entrusted by Plaintiff and the Class to safeguard their personal data, Defendant had a special relationship with Plaintiff and the Class. Plaintiff and the Class agreed to provide their personal data with the understanding that Defendant would take appropriate measures to protect it and would inform Plaintiff and the Class of any security concerns that might call for action by Plaintiff and the Class.

86. Kraemer breached its duty to Plaintiff and the Class by failing to implement and maintain reasonable security controls that were capable of adequately protecting the PII of Plaintiff and the Class.

87. Kraemer also breached its duty to timely and accurately disclose to its clients and employees, Plaintiff and the Class, that their PII had been or was reasonably believed to have been improperly accessed or stolen.

88. Kraemer's negligence in failing to maintain reasonable data security is further evinced by its failure to comply with legal obligations and industry standards, and the delay between the date of the Data Breach and the time when Kraemer disclosed it.

89. The injuries to Plaintiff and the Class were reasonably foreseeable to Kraemer because laws and statutes, and industry standards require it to safeguard and protect its computer systems and employ procedures and controls to ensure that unauthorized third parties did not gain access to Plaintiff's and the Class's PII.

90. The injuries to Plaintiff and the Class were reasonably foreseeable because Kraemer knew or should have known that systems used for safeguarding PII were inadequately secured and exposed consumer PII to being breached, accessed, and stolen by hackers and unauthorized third parties. As such, Kraemer's own misconduct created a foreseeable risk of harm to Plaintiff and the Class.

91. Kraemer implemented knowingly deficient data security measures and failed to adopt reasonable measure that could protect the PII of Plaintiff and the Class, and those deficient security measures proximately caused Plaintiff's and the Class's injuries because they directly allowed hackers to easily access Plaintiff and the Class's PII. This ease of access allowed the hackers to steal PII of Plaintiff and the Class, which could lead to dissemination in black markets.

92. As a direct proximate result of Kraemer's conduct, Plaintiff and the Class have suffered theft of their PII. Kraemer allowed thieves access to Plaintiff's and the Class's PII, thereby decreasing the security of Plaintiff's and the Class's financial and health accounts, making Plaintiff's and the Class's identities less secure and reliable, and subjecting Plaintiff and the Class to the imminent threat of identity theft. Not only will Plaintiff and the Class have to incur time and money to re-secure their bank accounts and identities, but they will also have to protect against identity theft for years to come.

SECOND CAUSE OF ACTION
Negligence Per Se
(On Behalf of Plaintiff and the Class)

93. Plaintiff incorporates by reference all previous allegations as though fully set forth herein.

94. Kraemer's unreasonable data security measures and failure to timely notify Plaintiff and the Class of the Data Breach violates Section 5 of the FTC Act. Although the FTC Act does not create a private right of action, it requires businesses to institute reasonable data security measures and breach notification procedures, which Kraemer failed to do.

95. Section 5 of the FTCA, 15 U.S.C. § 45, prohibits "unfair. . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice of businesses like Kraemer failing to use reasonable measures to protect sensitive data. The FTC publications and orders described above also form the basis of Kraemer's duty.

96. Kraemer violated Section 5 of the FTC Act by failing to use reasonable measures to protect sensitive data and by not complying with applicable industry standards. Kraemer's conduct was particularly unreasonable given the foreseeable consequences of a Data Breach should Kraemer employ unreasonable, inadequate data security.

97. Kraemer's violation of Section 5 of the FTC Act constitutes negligence per se.

98. Plaintiff and the Class are within the class of persons Section 5 of the FTCA (and similar state statutes) were intended to protect. Additionally, the harm that has occurred is the type of harm the FTC Act (and similar state statutes) was intended to guard against. The FTC has pursued over fifty 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 type of harm suffered by Plaintiff and the Class.

99. As a direct and proximate result of Kraemer's negligence per se, Plaintiff and the Class have suffered and continue to suffer injury.

THIRD CAUSE OF ACTION
Declaratory Judgment
(On Behalf of Plaintiff and the Class)

100. Plaintiff incorporates by reference all previous allegations as though fully set forth herein.

101. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, et seq., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and to grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as those alleged herein, which are tortious, and which violate the terms of the federal and state statutes described above.

102. An actual controversy has arisen in the wake of the Data Breach at issue regarding Kraemer's common law and other duties to act reasonably with respect to employing reasonable data security. Plaintiff alleges that Kraemer's actions in this respect were inadequate and unreasonable and, upon information and belief, remain inadequate and unreasonable. Additionally, Plaintiff and the Class continue to suffer injury due to the continued and ongoing threat of new or additional fraud against them or on their accounts using the stolen data.

103. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Kraemer owed, and continues to owe, a legal duty to employ reasonable data security to secure the PII with which it is entrusted, specifically including the PII of its employees, and to notify impacted individuals of the Data Breach under the common law and Section 5 of the FTC Act;

b. Kraemer breached, and continues to breach, its duty by failing to employ reasonable measures to secure its employees' personal and financial information; and

c. Kraemer's breach of its legal duty continues to cause harm to Plaintiff and the Class.

104. The Court should also issue corresponding injunctive relief requiring Kraemer to employ adequate security protocols consistent with industry standards to protect its clients' (i.e., Plaintiff's and the Class's) data.

105. If an injunction is not issued, Plaintiff and the Class will suffer irreparable injury and lack an adequate legal remedy in the event of another breach of Kraemer's data systems. If another breach of Kraemer's data systems occurs, Plaintiff and the Class will not have an adequate remedy at law because many of the resulting injuries are not readily quantified in full and they will be forced to bring multiple lawsuits to rectify the same conduct. Simply put, monetary damages, while warranted to compensate Plaintiff and the Class for their out-of-pocket and other damages that are legally quantifiable and provable, do not cover the full extent of injuries suffered by Plaintiff and the Class, which include monetary damages that are not legally quantifiable or provable.

106. The hardship to Plaintiff and the Class if an injunction is not issued exceeds the hardship to Kraemer if an injunction is issued.

107. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach, thus eliminating the injuries that would result to Plaintiff, the Class, and the public at large.

FOURTH CAUSE OF ACTION
Breach of an Implied Contract
(On Behalf of Plaintiff and the Class)

108. Plaintiff and members of the Class incorporate the above allegations as if fully set forth herein.

109. Kraemer offered to employ Plaintiff and members of the Class in exchange for their PII.

110. Plaintiff and the Class entrusted their PII to Defendant at the time they entered into an employment relationship with Defendant. In so doing, Plaintiff and the Class entered into implied contracts with Defendant by which Defendant agreed, based on its representations and actions to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and the Class if their data had been breached and compromised or stolen.

111. Kraemer agreed they would not disclose the PII it collects to unauthorized persons. Kraemer also promised to safeguard PII.

112. Plaintiff and the Class accepted Kraemer's offers by disclosing their PII to Kraemer in exchange for employment with Kraemer.

113. Plaintiff and the Class fully performed their obligations under the implied contracts with Defendant.

114. Implicit in the parties' agreement was that Kraemer would provide Plaintiff and the Class with prompt and adequate notice of all unauthorized access and/or theft of their PII.

115. Plaintiff and the Class would not have entrusted their PII to Kraemer in the absence of such agreement with Kraemer.

116. Kraemer materially breached the contract(s) it had entered with Plaintiff and the Class by failing to safeguard such information and failing to notify them promptly of the Data Breach that compromised such information. Kraemer further breached the implied contracts with Plaintiff and the Class by:

a. Failing to properly safeguard and protect Plaintiff and members of the Class's PII;

b. Failing to comply with industry standards as well as legal obligations that are necessarily incorporated into the parties' agreement; and

c. Failing to ensure the confidentiality and integrity of PII that Kraemer created, received, maintained, and transmitted.

117. The damages sustained by Plaintiff and the Class as described above were the direct and proximate result of Kraemer's material breaches of their agreement(s).

118. Plaintiff and the Class have performed as required under the relevant agreements, or such performance was waived by the conduct of Kraemer.

119. The covenant of good faith and fair dealing is an element of every contract. All such contracts impose upon each party a duty of good faith and fair dealing. The parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—not merely the letter—of the bargain. Put differently, the

parties to a contract are mutually obligated to comply with the substance of their contract in addition to its form.

120. Subterfuge and evasion violate the obligation of good faith in performance even when an actor believes their conduct to be justified. Bad faith may be overt or may consist of inaction, and fair dealing may require more than honesty.

121. Kraemer failed to advise Plaintiff and the Class of the Data Breach promptly and sufficiently.

122. In these and other ways, Kraemer violated its duty of good faith and fair dealing.

123. Plaintiff and the Class have sustained damages because of Kraemer's breaches of its agreement, including breaches thereof through violations of the covenant of good faith and fair dealing.

FIFTH CAUSE OF ACTION
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

124. Plaintiff and the Class incorporate the above allegations as if fully set forth herein.

125. This claim is pleaded in the alternative to the breach of implied contractual duty claim.

126. Plaintiff and Class Members conferred a monetary benefit on Defendant, by providing Defendant with their valuable PII. They also conferred a benefit on Defendant by providing their employment services.

127. Kraemer appreciated or had knowledge of the benefits conferred upon them by Plaintiff and the Class. Kraemer also benefited from the receipt of Plaintiff's and members of the Class's PII, as this was used to provide its goods and services.

128. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class Members' PII and by retaining the benefit of Plaintiff's and the Class's labor.

129. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to avoid its data security obligations at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

130. Under principals of equity and good conscience, Kraemer should not be permitted to retain the full value of Plaintiff and the d Class's services and their PII because Kraemer failed to adequately protect their PII. Plaintiff and the Class would not have provided their PII to Kraemer had they known Kraemer would not adequately protect their PII.

131. Kraemer should be compelled to disgorge into a common fund for the benefit of Plaintiff and the Class all unlawful or inequitable proceeds received by it because of its misconduct and Data Breach.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually, and on behalf of all others similarly situated, respectfully requests that the Court enter an order:

a. Certifying this case as a class action on behalf of Plaintiff and the proposed Class, appointing Plaintiff as class representative, and appointing his counsel to represent the Class;

b. Finding that Defendant engaged in the unlawful conduct as alleged herein;

c. Enjoining Defendant's conduct and requiring Defendant to implement proper data security practices, specifically:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state, or local laws;

iii. requiring Defendant to delete, destroy, and purge the PII of Plaintiff and the Class unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and the Class;

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the personal identifying information of Plaintiff's and the Class's PII;

vi. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

ix. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

x. requiring Defendant to conduct regular database scanning and securing checks;

xi. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling PII, as well as protecting the PII of Plaintiff and the Class;

xii. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and

periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting PII;

xiv. requiring Defendant implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Defendant to meaningfully educate all Class members about the threats that they face as a result of the loss of their confidential PII to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers;

xvii. for a period of 10 years, appointing a qualified and independent third-party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the Class and Subclasses, and to report any deficiencies with compliance of the Court's final judgment;

xviii. requiring Defendant to design, maintain, and test its computer systems to ensure that PII in its possession is adequately secured and protected;

xix. requiring Defendant to disclose any future data breaches in a timely and accurate manner;

xx. requiring Defendant to implement multi-factor authentication requirements;

xxi. requiring Defendant' employees to change their passwords on a timely and regular basis, consistent with best practices; and

xxii. requiring Defendant to provide lifetime credit monitoring and identity theft repair services to Class members.

a. Awarding Plaintiff and the Class damages;

b. Awarding Plaintiff and Class pre-judgment and post-judgment interest on all amounts awarded;

c. Awarding Plaintiff and the Class reasonable attorneys' fees, costs, and expenses; and

d. Granting such other relief as the Court deems just and proper.

JURY TRIAL DEMANDED

132. Plaintiff and the Class demand a trial by jury on all issues so triable.

Dated: June 20, 2023

TURKE & STRAUSS LLP

By: */s/ Raina C. Borrelli*

Raina C. Borrelli (MN No: 0392127)
raina@turkestrauss.com
Samuel J. Strauss (*pro hac vice*)
sam@turkestrauss.com
Brittany Resch (MN No: 0397656)
brittanyr@turkestrauss.com
613 Williamson St., Suite 201
Madison, WI 53703
Telephone (608) 237-1775
Facsimile: (608) 509-4423

Attorneys for Plaintiff and Proposed Class

ClassAction.org
