Exhibit A

UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF TEXAS
HOUSTON DIVISION

JOSEPH TROTTIER, individually and on behalf of all others similarly situated, Plaintiffs, vs. SYSCO CORPORATION, Defendant.	**Case No. 4:23-cv-01818** **Consolidated Cases:** **4:23-cv-01831** **4:23-cv-01845** **4:23-cv-02388** **4:23-cv-02547** **JURY TRIAL DEMANDED**

CONSOLIDATED AMENDED CLASS ACTION COMPLAINT

INTRODUCTION

1. Plaintiffs Joseph Trottier, Carmelo Pacheco, Bryce Miller, and Angela Cooks (collectively, "Plaintiffs" or "Representative Plaintiffs"), bring this class action against Defendant Sysco Corporation ("Defendant") for its failure to properly secure and safeguard Representative Plaintiffs' and Class Members' personally identifiable information stored within Defendant's information network, including without limitation name, Social Security numbers, and account numbers (these types of information, *inter alia*, being hereafter referred to, collectively, as "personally identifiable information" or "PII").[1] Defendant failed to properly secure and safeguard Representative Plaintiffs' and Class Members' PII stored within Defendant's information network.

[1] Personally identifiable information ("PII") generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual. PII also is generally defined to include certain identifiers that do not on its face name an individual, but that are considered to be particularly sensitive and/or valuable if in the wrong hands (for example, Social Security numbers, passport numbers, driver's license numbers, financial account numbers, etc.).

2. With this action, Representative Plaintiffs seek to hold Defendant responsible for the harms it caused and will continue to cause Representative Plaintiffs and countless other similarly situated persons in the massive and preventable cyberattack purportedly discovered by Defendant on March 5, 2023, by which cybercriminals infiltrated Defendant's inadequately protected network servers and accessed highly sensitive PII, which was being kept unprotected (the "Data Breach").

3. On or before May 27, 2023, reports surfaced on the Internet that the Dark Angel / Dunghill ransomware group obtained more than 10 terabytes of data during the Data Breach.

4. On or before July 31, 2023, reports surfaced on the Internet that the Dark Angel / Dunghill ransomware group had posted data exfiltrated during the Data Breach on the dark web, including (i) screenshots of files available, (ii) a detailed list of files and content available, and (iii) download links to exfiltrated data dump files.

5. Prior to the Data Breach, Defendant published on its website a "Sysco Applicant Privacy Notice" directed to job applicants that included the following promises regarding data security:

> HOW WE PROTECT PERSONAL DATA
>
> We have put in place appropriate security measures to prevent your personal data from being accidentally lost, used or accessed in an unauthori[z]ed way, altered or disclosed. In addition, we limit access to your personal data to those employees, agents, contractors and other third parties who have a business need-to-know. They will only process your personal data on our instructions, and they are subject to a duty of confidentiality.
>
> We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach

where we are legally required to do so.

6. While Defendant claims to have discovered the breach as early as March 5, 2023, Defendant failed to inform Representative Plaintiffs until May 5, 2023, vis-à-vis a mailed letter.

7. Defendant acquired, collected and stored Representative Plaintiffs' and Class Members' PII in connection with their employment by Defendant. Therefore, at all relevant times, Defendant knew or should have known that its networks held Representative Plaintiffs' and Class Members' sensitive data, including highly confidential PII.

8. By obtaining, collecting, using and deriving a benefit from Representative Plaintiffs' and Class Members' PII, Defendant assumed legal and equitable duties to those individuals. These duties arise from state and federal statutes and regulations as well as common law principles.

9. Defendant disregarded the rights of Representative Plaintiffs and Class Members by intentionally, willfully, recklessly or negligently failing to take and implement adequate and reasonable measures to ensure that Representative Plaintiffs' and Class Members' PII was safeguarded; failing to take available steps to prevent an unauthorized disclosure of data; and failing to follow applicable, required, and appropriate protocols, policies, and procedures regarding the encryption of data, even for internal use. As a result, the PII of Representative Plaintiffs and Class Members was compromised through disclosure to an unknown and unauthorized third party—an undoubtedly nefarious third party that seeks to profit off this disclosure by defrauding Representative Plaintiffs and Class Members in the future. Representative Plaintiffs and Class Members have a continuing interest in ensuring that their information is and remains safe, and they are entitled to injunctive and other equitable relief.

JURISDICTION AND VENUE

10. Jurisdiction is proper in this Court under 28 U.S.C. §1332 (diversity jurisdiction). Specifically, this Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action where the amount in controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class and at least one other Class Member is a citizen of a state different from Defendant.

11. Supplemental jurisdiction to adjudicate issues pertaining to state law is proper in this Court under 28 U.S.C. § 1367.

12. Defendant Sysco Corporation is a Delaware corporation headquartered and has its principal place of business in Houston, Texas. Defendant also has sufficient minimum contacts in Texas and has intentionally availed itself of this jurisdiction by marketing and selling products and services and by accepting and processing payments for those products and services within Texas. Sysco Corporation is a citizen of Texas.

13. Venue is proper in this Court under 28 U.S.C. § 1391 because a substantial part of the events that gave rise to Representative Plaintiffs' claims took place within the Houston Division of the Southern District of Texas, and Defendant does business and has its headquarters and principal place of business there.

PLAINTIFFS

14. Plaintiff Trottier is a citizen and resident of the state of Wisconsin.

15. Plaintiff Pacheco is a citizen and resident of the state of Pennsylvania.

16. Plaintiff Miller is a citizen and resident of the state of Tennessee.

17. Plaintiff Cooks is a citizen and resident of the state of Kansas.

18. Defendant received highly sensitive personal information from Plaintiffs. As a

result, Representative Plaintiffs' information was among the data accessed by an unauthorized third party in the Data Breach.

19. At all times herein relevant, Representative Plaintiffs are (or were) members of the Class.

20. As required to obtain employment from Defendant, Representative Plaintiffs provided Defendant with highly sensitive personal information.

21. Representative Plaintiffs' PII was exposed in the Data Breach because Defendant stored and/or shared Representative Plaintiffs' PII. Their PII was within the possession and control of Defendant at the time of the Data Breach.

22. Representative Plaintiffs received letters from Defendant, in or about May 2023, informing them that their PII was involved in the Data Breach (the "Notice").

23. As a result, Representative Plaintiffs spent uncompensated time dealing with the consequences of the Data Breach, which included and continues to include, time spent verifying the legitimacy and impact of the Data Breach, exploring credit monitoring and identity theft insurance options, self- monitoring their accounts and seeking legal counsel regarding their options for remedying and/or mitigating the effects of the Data Breach. This uncompensated time has been lost forever and cannot be recaptured.

24. Representative Plaintiffs suffered actual injury in the form of damages to and diminution in the value of their PII—a form of intangible property that they entrusted to Defendant, which was compromised in and as a result of the Data Breach.

25. Representative Plaintiffs suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and have anxiety and increased concerns for the loss of their privacy, as well as anxiety over the impact of cybercriminals accessing, using and selling

their PII.

26. Representative Plaintiffs have suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft and misuse resulting from their PII being placed in the hands of unauthorized third parties/criminals.

27. Representative Plaintiffs have a continuing interest in ensuring that their PII, which upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

DEFENDANT

28. Defendant Sysco Corporation is a corporation with its headquarters and principal place of business located at 1390 Enclave Parkway, Houston, TX 77077, which is in the Houston Division of the Southern District of Texas. Sysco Corporation is a citizen of Texas. Sysco Corporation can be served with process at Corporation Service Company d/b/a CSC-Lawyers Incorporating Service Company, 211 E. 7th Street, Suite 620, Austin, TX 78701.

29. According to Defendant's website, "Sysco is the global leader in selling, marketing and distributing food products to restaurants, healthcare and educational facilities, lodging establishments and other customers who prepare meals away from home. Its family of products also includes equipment and supplies for the food service and hospitality industries."[2]

30. The true names and capacities of persons or entities, whether individual, corporate, associate or otherwise, if any, who may be responsible for some of the claims alleged here are currently unknown to Representative Plaintiffs. Representative Plaintiffs will seek leave of court to amend this Complaint to reflect the true names and capacities of such other responsible parties

[2] Our Purpose: https://www.sysco.com/about/company-profile/our-purpose (last accessed February 14, 2024)

when its identities become known.

CLASS ACTION ALLEGATIONS

31. Representative Plaintiffs bring this action pursuant to the provisions of Rules 23(a), (b)(2), and (b)(3) of the Federal Rules of Civil Procedure, on behalf of themselves and the following Class (collectively, the "Class"):

> **Nationwide Class:**
> "All individuals within the United States of America whose PII was exposed to unauthorized third parties as a result of the Data Breach discovered by Defendant on March 5, 2023."

32. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors and any entity in which Defendant has a controlling interest, all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out, any and all federal, state or local governments, including but not limited to its departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

33. Representative Plaintiffs reserve the right to amend the above definition or to propose subclasses in subsequent pleadings and motions for class certification.

34. This action has been brought and may properly be maintained as a class action under Federal Rule of Civil Procedure Rule 23 because there is a well-defined community of interest in the litigation and membership in the proposed classes is easily ascertainable.

a. **Numerosity:** A class action is the only available method for the fair and efficient adjudication of this controversy. The members of the Plaintiff Class are so

numerous that joinder of all members is impractical, if not impossible. According to the breach report submitted to the Office of the Maine Attorney General, at least 126,000 individuals were impacted in the Data Breach.[3]

b. **Commonality:** Representative Plaintiffs and the Class Members share a community of interests in that there are numerous common questions and issues of fact and law which predominate over any questions and issues solely affecting individual members, including but not necessarily limited to:

1) Whether Defendant had a legal duty to Representative Plaintiffs and the Class to exercise due care in collecting, storing, using and/or safeguarding their PII;

2) Whether Defendant knew or should have known of the susceptibility of its data systems to a data breach;

3) Whether Defendant's security procedures and practices to protect its systems were reasonable in light of the measures recommended by data security experts;

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

5) Whether Defendant's failure to implement adequate data security measures allowed the Data Breach to occur;

6) Whether Defendant failed to comply with its own policies and

[3] https://apps.web.maine.gov/online/aeviewer/ME/40/28ded7f7-4f72-4a32-b531-1ba31469d1aa.shtml

applicable laws, regulations, and industry standards relating to data security;

7) Whether Defendant adequately, promptly, and accurately informed Representative Plaintiffs and Class Members that their PII had been compromised;

8) How and when Defendant actually learned of the Data Breach;

9) Whether Defendant's conduct, including its failure to act, resulted in or was the proximate cause of the breach of its systems, resulting in the loss of the PII of Representative Plaintiffs and Class Members;

10) Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

11) Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Representative Plaintiffs and Class Members;

12) Whether Representative Plaintiffs and Class Members are entitled to actual and/or statutory damages and/or whether injunctive, corrective and/or declaratory relief and/or an accounting is/are appropriate as a result of Defendant's wrongful conduct;

13) Whether Representative Plaintiffs and Class Members are entitled to restitution as a result of Defendant's wrongful conduct.

c. **Typicality:** Representative Plaintiffs' claims are typical of the claims of the Class. Representative Plaintiffs and all members of the Class sustained damages arising out of and caused by Defendant's common course of conduct in violation of law, as alleged herein.

d. **Adequacy of Representation:** Representative Plaintiffs in this class action are adequate representatives of each of the Class in that the Representative Plaintiffs have the same interest in the litigation of this case as the Class Members, are committed to vigorous prosecution of this case and have retained competent counsel who are experienced in conducting litigation of this nature. Representative Plaintiffs are not subject to any individual defenses unique from those conceivably applicable to other Class Members or the Class in its entirety. Representative Plaintiffs anticipate no management difficulties in this litigation.

e. **Superiority of Class Action:** Since the damages suffered by individual Class Members while not inconsequential, may be relatively small, the expense and burden of individual litigation by each member makes or may make it impractical for members of the Class to seek redress individually for the wrongful conduct alleged herein. Should separate actions be brought or be required to be brought, by each individual member of the Class, the resulting multiplicity of lawsuits would cause undue hardship and expense for the Court and the litigants. The prosecution of separate actions would also create a risk of inconsistent rulings which might be dispositive of the interests of other Class Members who are not parties to the adjudications and/or may substantially impede their ability to adequately protect their interests.

35. This Class Action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to Class Members, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class in its entirety. Defendant's

policies and practices challenged herein apply to and affect Class Members uniformly and Representative Plaintiffs' challenge of these policies and practices hinges on Defendant's conduct with respect to the Class in its entirety, not on facts or law applicable only to Representative Plaintiffs.

36. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the PII of Class Members, and Defendant may continue to act unlawfully as set forth in this Complaint.

37. Further, Defendant has acted or refused to act on grounds generally applicable to the Class and accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

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

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

b. Whether Defendant breached a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;

c. Whether Defendant failed to comply with its own policies and

applicable laws, regulations, and industry standards relating to data security;

d. Whether an implied contract existed between Defendant on the one hand, and Plaintiffs and Class Members on the other, and the terms of that implied contract;

e. Whether Defendant breached the implied contract;

f. Whether Defendant adequately and accurately informed Plaintiffs and Class Members that their PII had been compromised;

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

h. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Plaintiffs and Class Members; and,

i. Whether Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief as a result of Defendant's wrongful conduct.

COMMON FACTUAL ALLEGATIONS

The Cyberattack

39. In or about May 2023, Defendant sent Plaintiffs and Class Members a notice of the Data Breach (the "Notice of Data Breach"). Defendant informed Plaintiffs and Class Members that:

Sysco was recently the target of a cybersecurity event in which

> personal information for some of our current and former colleagues may have been impacted. First and foremost, I apologize that this happened and regret any concern this may cause. We value the trust you place in us to protect your privacy and take our responsibility to safeguard your personal information seriously.
>
> Please read below for additional information about what happened, the steps we are taking, as well as steps you can take to protect your information.
>
> Sysco has provided for you, free of charge, two years' worth of identity theft protection and credit monitoring….
>
> **What Happened?** On March 5, 2023, Sysco became aware of a cybersecurity event perpetrated by a threat actor believed to have begun on January 14, 2023, in which the threat actor gained access to our systems without authorization and claimed to have acquired certain data. While we have not yet fully validated these claims, we have determined that personal information for some of our current and former colleagues has been impacted.
>
> **What Information Was Involved?** While we cannot confirm at this time specifically what information may have been impacted for each individual colleague, we believe it could include some combination of the following data: personal information provided to Sysco for payroll purposes, including name, social security number, account numbers or similar information.

40. Thus, Defendant admitted in the Notice of Data Breach that one or more unauthorized third parties accessed Class Members' sensitive data including but not limited to name, date of birth, Social Security number and address. Representative Plaintiffs were among the individuals whose data was accessed in the Data Breach.

41. Representative Plaintiffs were provided the information detailed above upon their receipt of a letter from Defendant, dated in or about May 2023. They were not aware of the Data Breach until receiving that letter.

42. The details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure a breach does not occur again have not been shared

with Plaintiffs and Class Members, who retain a vested interest in ensuring that their information remains protected.

Defendant's Failed Response to the Breach

43. Not until roughly two months after they claimed to have discovered the Data Breach did Defendant begin sending the Notice to persons whose PII and/or financial information Defendant confirmed was potentially compromised as a result of the Data Breach. Importantly, Defendant did not inform Representative Plaintiffs and other the victims of the Data Breach until May 5, 2023, in a mailed Notice. The Notice provided basic details of the Data Breach and Defendant's recommended next steps.

44. The Notice included, inter alia, that Defendant had learned of the Data Breach on March 5, 2023, had taken steps to respond and were continuing to investigate. Defendant claimed that they took measures to protect against future attacks.

45. Upon information and belief, the unauthorized third-party cybercriminals gained access to Representative Plaintiffs' and Class Members' PII with the intent of engaging in misuse of the PII, including marketing and selling Representative Plaintiffs' and Class Members' PII.

46. Defendant had and continues to have obligations created by reasonable industry standards, common law, state statutory law and their own assurances and representations to keep Representative Plaintiffs' and Class Members' PII confidential and to protect such PII from unauthorized access.

47. Representative Plaintiffs and Class Members were required to provide their PII to Defendant in order to receive employment. Defendant acquired, collected, and stored Representative Plaintiffs' and Class Members' PII with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information

confidential and secure from unauthorized access.

48. Despite this, Representative Plaintiffs and the Class Members remain, even today, in the dark regarding what particular data was stolen, the particular malware used and what steps are being taken, if any, to secure their PII. Representative Plaintiffs and Class Members are left to speculate as to whether their PII was stolen and by whom. They are left to further speculate as to the full impact of the Data Breach and how exactly Defendant intends to enhance its information security systems and monitoring capabilities so as to prevent further breaches.

49. Representative Plaintiffs' and Class Members' PII may end up for sale on the Dark Web, or simply fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of Representative Plaintiffs and/or Class Members. Either way, unauthorized individuals can now easily access the PII of Representative Plaintiff and Class Members.

Defendant Collected/Stored Class Members' PII

50. Defendant acquired, collected and stored and assured reasonable security over Representative Plaintiffs' and Class Members' PII.

51. As a condition of their relationships with Representative Plaintiffs and Class Members, Defendant required that Representative Plaintiffs and Class Members entrust Defendant with highly sensitive and confidential PII.

52. By obtaining, collecting, and storing Representative Plaintiffs' and Class Members' PII, Defendant assumed legal and equitable duties and knew or should have known that it was thereafter responsible for protecting Representative Plaintiffs' and Class Members' PII from unauthorized disclosure.

53. Representative Plaintiffs and Class Members have taken reasonable steps to

maintain the confidentiality of their PII. Representative Plaintiffs and Class Members relied on Defendant to keep their PII confidential and securely maintained, to use this information for business and healthcare purposes only and to make only authorized disclosures of this information.

54. Defendant could have prevented the Data Breach, which they discovered as early as March 5, 2023, by properly securing and encrypting and/or more securely encrypting their servers generally as well as Representative Plaintiffs' and Class Members' PII.

55. Specifically, Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information it was maintaining for Plaintiffs and Class Members, causing the exposure of PII for Plaintiff and Class Members.

56. Defendant's negligence in safeguarding Representative Plaintiffs' and Class Members' PII is exacerbated by repeated warnings and alerts directed to protecting and securing sensitive data, as evidenced by the trending data breach attacks in recent years.

57. There have been a large number of high-profile cyberattacks even in just the short period preceding the filing of this Complaint and cyberattacks, generally, have become increasingly more common.

58. Due to the high-profile nature of data breaches, Defendant was and/or certainly should have been on notice and aware of such attacks occurring and, therefore, should have assumed and adequately performed the duty of preparing for such an imminent attack. This is especially true given that Defendant is a large, sophisticated operation with the resources to put adequate data security protocols in place.

59. Yet, despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect Representative

Plaintiffs' and Class Members' PII and financial information from being compromised.

Defendant Had an Obligation to Protect the Stolen Information

60. Defendant's failure to adequately secure Representative Plaintiffs' and Class Members' sensitive information, breaches duties it owes Representative Plaintiffs and Class Members under statutory and common law.

61. Defendant was prohibited by the Federal Trade Commission Act (the "FTC Act") (15 U.S.C. § 45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission (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 the FTC Act. *See, e.g.*, *FTC v. Wyndham Worldwide Corp*., 799 F.3d 236 (3d Cir. 2015).

62. In addition to its obligations under federal and state laws, Defendant owed a duty to Representative Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting the PII in Defendant's possession from being compromised, lost, stolen, accessed and misused by unauthorized persons. Defendant owed a duty to Representative 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 PII of Representative Plaintiffs and Class Members.

63. Defendant owed a duty to Representative Plaintiffs and Class Members to design, maintain, and test its computer systems, servers and networks to ensure that the PII in its possession was adequately secured and protected.

64. Defendant owed a duty to Representative Plaintiffs and Class Members to create

and implement reasonable data security practices and procedures to protect the PII in its possession including not sharing information with other entities who maintained sub-standard data security systems.

65. Defendant owed a duty to Representative Plaintiffs and Class Members to implement processes that would immediately detect a breach on its data security systems in a timely manner.

66. Defendant owed a duty to Representative Plaintiffs and Class Members to act upon data security warnings and alerts in a timely fashion.

67. Defendant owed a duty to Representative Plaintiffs and Class Members to disclose if its computer systems and data security practices were inadequate to safeguard individuals' PII from theft because such an inadequacy would be a material fact in the decision to entrust this PII to Defendant.

68. Defendant owed a duty of care to Representative Plaintiffs and Class Members because they were foreseeable and probable victims of any inadequate data security practices.

69. Defendant owed a duty to Representative Plaintiffs and Class Members to encrypt and/or more reliably encrypt Representative Plaintiffs' and Class Members' PII and monitor user behavior and activity in order to identity possible threats.

Value of the Relevant Sensitive Information

70. PII is a valuable commodity for which a "cyber black market" exists in which criminals openly post stolen payment card numbers, Social Security numbers and other personal information on a number of underground internet websites. Unsurprisingly, PII is at high risk for theft and acutely affected by cyberattacks.

71. The high value of PII to criminals is further evidenced by the prices they will pay through the Dark Web. Numerous sources cite Dark Web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[4] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the Dark Web.[5] Criminals can also purchase access to entire company data breaches from $999 to $4,995.[6]

72. These criminal activities have and will result in devastating financial and personal losses to Representative Plaintiffs and Class Members. For example, it is believed that certain PII compromised in the 2017 Experian data breach was being used three years later by identity thieves to apply for COVID-19-related benefits in the state of Oklahoma. Such fraud will be an omnipresent threat for Representative Plaintiffs and Class Members for the rest of their lives. They will need to remain constantly vigilant.

73. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification

---

[4] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed July 28, 2021).

[5] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last accessed November 5, 2021).

[6] *In the Dark*, VPN Overview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed January 21, 2022).

number."

74. Identity thieves can use PII, such as that of Representative Plaintiffs and Class Members which Defendant failed to keep secure, to perpetrate a variety of crimes that harm victims. For instance, identity thieves may commit various types of government fraud such as immigration fraud, obtaining a driver's license or identification card in the victim's name but with another's picture, using the victim's information to obtain government benefits or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund.

75. The ramifications of Defendant's failure to keep secure Representative Plaintiff's and Class Members' PII are long lasting and severe. Once PII is stolen, particularly identification numbers, fraudulent use of that information and damage to victims may continue for years. Indeed, the PII of Representative Plaintiffs and Class Members was taken by hackers to engage in identity theft or to sell it to other criminals who will purchase the PII for that purpose. The fraudulent activity resulting from the Data Breach may not come to light for years.

76. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [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.[7]

77. When cybercriminals access personally sensitive data—as they did here—there is

[7] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* http://www.gao.gov/new.items/d07737.pdf (last accessed January 21, 2022).

no limit to the amount of fraud to which Defendant may have exposed Representative Plaintiffs and Class Members.

78. And data breaches are preventable.[8] As Lucy Thompson wrote in the Data Breach And Encryption Handbook, "[i]n almost all cases, the Data Breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions."[9] She added that "[o]rganizations that collect, use, store and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised "[10]

79. Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules and procedures … "Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a data breach never occurs."[11]

80. Here, Defendant knew of the importance of safeguarding PII and of the foreseeable consequences that would occur if Representative Plaintiffs' and Class Members' PII was stolen, including the significant costs that would be placed on Representative Plaintiffs and Class Members as a result of a breach of this magnitude. As detailed above, Defendant is a large, sophisticated organization with the resources to deploy robust cybersecurity protocols. It knew or should have known that the development and use of such protocols were necessary to fulfill its statutory and common law duties to Representative Plaintiffs and Class Members. Its failure to do so is therefore intentional, willful, reckless, negligent and/or grossly negligent.

---

[8] Lucy L. Thompson, "Despite the Alarming Trends, Data Breaches Are Preventable," *in* DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012).
[9] *Id.* at 17.
[10] *Id.* at 28.
[11] *Id.*

81. Defendant disregarded the rights of Representative Plaintiffs and Class Members by, inter alia, (i) intentionally, willfully, recklessly or negligently failing to take adequate and reasonable measures to ensure that its network servers were protected against unauthorized intrusions, (ii) failing to disclose that it did not have adequately robust security protocols and training practices in place to adequately safeguard Representative Plaintiffs' and Class Members' PII, (iii) failing to take standard and reasonably available steps to prevent the Data Breach, (iv) concealing the existence and extent of the Data Breach for an unreasonable duration of time, and (v) failing to provide Representative Plaintiffs and Class Members prompt and accurate notice of the Data Breach.

Plaintiff Trottier's Experience

82. Plaintiff Trottier has been an employee of Sysco as a Truck Driver in Wisconsin.

83. As a result of the Data Breach, Plaintiff Trottier's sensitive information was accessed and/or acquired by an unauthorized actor. The confidentiality of Plaintiff Trottier's sensitive information has been irreparably harmed. For the rest of his life, Plaintiff Trottier will have to worry about when and how his sensitive information may be shared or used to his detriment.

84. As a result of the Data Breach notice, Plaintiff Trottier spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach and self-monitoring his accounts. This time has been lost forever and cannot be recaptured.

85. Additionally, Plaintiff Trottier is very careful about sharing his sensitive PII. He has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

86. Plaintiff Trottier stores any documents containing his sensitive PII in a safe and secure location or destroys the documents. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

87. Plaintiff Trottier suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy.

88. Plaintiff Trottier has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII, especially his Social Security number, being placed in the hands of unauthorized third parties and possibly criminals.

89. Plaintiff Trottier 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 future breaches.

Plaintiff Miller's Experience

90. Plaintiff Miller worked for Defendant prior to the Data breach and received Defendant's Notice of Data Breach, dated May 11, 2023, on or about that date. The notice stated that Plaintiff's personal information was impacted by the Data Breach.

91. As a result of the Data Breach, Plaintiff Miller's sensitive information may have been accessed and/or acquired by an unauthorized actor. The confidentiality of Plaintiff Miller's sensitive information has been irreparably harmed. For the rest of his life, Plaintiff Miller will have to worry about when and how his sensitive information may be shared or used to his detriment.

92. As a result of the Data Breach notice, Plaintiff Miller spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice

of Data Breach and self-monitoring his accounts. This time has been lost forever and cannot be recaptured.

93. Additionally, Plaintiff Miller is very careful about sharing his sensitive PII. He has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

94. Plaintiff Miller stores any documents containing his sensitive PII in a safe and secure location or destroys the documents. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

95. Plaintiff Miller suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy.

96. Plaintiff Miller has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII, especially his Social Security number, being placed in the hands of unauthorized third parties and possibly criminals.

97. Plaintiff Miller 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 future breaches.

Plaintiff Cooks' Experience

98. Plaintiff Cooks worked for Defendant prior to the Data breach and received Defendant's Notice of Data Breach, in or around early May, 2023. The notice stated that Plaintiff's personal information was impacted by the Data Breach.

99. As a result of the Data Breach, Plaintiff Cooks' sensitive information may have

been accessed and/or acquired by an unauthorized actor. The confidentiality of Plaintiff Cooks' sensitive information has been irreparably harmed. For the rest of her life, Plaintiff will have to worry about when and how her sensitive information may be shared or used to his detriment.

100. Plaintiff Cooks is a former Corrections Sergeant, having worked at a maximum-security prison in the state of Kansas. Because of this, having her information compromised and in the hands of criminals presents an especially high risk to the safety of her and her family, which could be life-threatening.

101. As a result of the Data Breach notice, Plaintiff Cooks spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach and self-monitoring her accounts. This time has been lost forever and cannot be recaptured.

102. Additionally, Plaintiff Cooks is very careful about sharing her sensitive PII. She has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

103. Plaintiff stores any documents containing her sensitive PII in a safe and secure location or destroys the documents. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

104. Plaintiff Cooks suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has fear and anxiety and increased concerns for the loss of her privacy.

105. Plaintiff Cooks has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PII, especially

her Social Security number and baking information, being placed in the hands of unauthorized third parties and possibly criminals.

106. Plaintiff Cooks has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Pacheco's Experience

107. Plaintiff Pacheco worked for Defendant prior to the Data breach and received Defendant's Notice of Data Breach, in or around early May, 2023. The notice stated that Plaintiff's personal information was impacted by the Data Breach.

108. As a result of the Data Breach, Plaintiff Pacheco's sensitive information may have been accessed and/or acquired by an unauthorized actor. The confidentiality of Plaintiff Pacheco's sensitive information has been irreparably harmed. For the rest of his life, Plaintiff Pacheco's will have to worry about when and how her sensitive information may be shared or used to his detriment.

109. As a result of the Data Breach notice, Plaintiff Pacheco spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach and self-monitoring her accounts. This time has been lost forever and cannot be recaptured.

110. Additionally, Plaintiff Pacheco is very careful about sharing his sensitive PII. He has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

111. Plaintiff Pacheco stores any documents containing his sensitive PII in a safe and

secure location or destroys the documents. Moreover, he diligently chooses unique usernames and passwords for her various online accounts.

112. Plaintiff Pacheco suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has fear and anxiety and increased concerns for the loss of his privacy.

113. Plaintiff Pacheco has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PII, especially her Social Security number and baking information, being placed in the hands of unauthorized third parties and possibly criminals.

114. Plaintiff Pacheco has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

FIRST CLAIM FOR RELIEF
Negligence
(On Behalf of Plaintiffs and the Class)

115. The allegations of the preceding paragraphs 1 through 114 is incorporated in this Cause of Action with the same force and effect as though fully set forth herein.

116. At all times herein relevant, Defendant owed Representative Plaintiffs and Class Members a duty of care, inter alia, to act with reasonable care to secure and safeguard their PII and to use commercially reasonable methods to do so. Defendant took on this obligation upon accepting and storing the PII of Representative Plaintiffs and Class Members in its computer systems and on its networks.

117. Among these duties, Defendant was expected:

a. to exercise reasonable care in obtaining, retaining, securing, safeguarding,

deleting and protecting the PII in its possession;

b. to protect Representative Plaintiffs' and Class Members' PII using reasonable and adequate security procedures and systems that were/are compliant with industry-standard practices;

c. to implement processes to quickly detect the Data Breach and to timely act on warnings about data breaches; and

d. to promptly notify Representative Plaintiffs and Class Members of any data breach, security incident or intrusion that affected or may have affected their PII.

118. Defendant knew that the PII was private and confidential and should be protected as private and confidential and, thus, Defendant owed a duty of care not to subject Representative Plaintiffs and Class Members to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices.

119. Defendant knew or should have known of the risks inherent in collecting and storing PII, the vulnerabilities of its data security systems and the importance of adequate security. Defendant knew about numerous, well-publicized data breaches.

120. Defendant knew or should have known that its data systems and networks did not adequately safeguard Representative Plaintiffs' and Class Members' PII.

121. Only Defendant was in the position to ensure that its systems and protocols were sufficient to protect the PII that Representative Plaintiffs and Class Members had entrusted to them.

122. Defendant breached its duties to Representative Plaintiffs and Class Members by failing to provide fair, reasonable or adequate computer systems and data security practices to safeguard the PII of Representative Plaintiffs and Class Members.

123. Because Defendant knew that a breach of its systems could damage thousands of individuals, including Representative Plaintiffs and Class Members, Defendant had a duty to adequately protect its data systems and the PII contained thereon.

124. Representative Plaintiffs' and Class Members' willingness to entrust Defendant with their PII was predicated on the understanding that Defendant would take adequate security precautions. Moreover, only Defendant had the ability to protect its systems and the PII it stored on them from attack. Thus, Defendant had a special relationship with Representative Plaintiffs and Class Members.

125. Defendant also had independent duties under state and federal laws that required Defendant to reasonably safeguard Representative Plaintiffs' and Class Members' PII and promptly notify them about the Data Breach. These "independent duties" are untethered to any contract between Defendant and Representative Plaintiffs and/or the remaining Class Members.

126. Defendant breached its general duty of care to Representative Plaintiffs and Class Members in, but not necessarily limited to, the following ways:

a. by failing to provide fair, reasonable or adequate computer systems and data security practices to safeguard the PII of Representative Plaintiffs and Class Members;

b. by failing to timely and accurately disclose that Representative Plaintiffs' and Class Members' PII had been improperly acquired or accessed;

c. by failing to adequately protect and safeguard the PII by knowingly disregarding standard information security principles, despite obvious risks and by allowing unmonitored and unrestricted access to unsecured PII;

d. by failing to provide adequate supervision and oversight of the PII and

financial information with which they were and are entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted an unknown third party to gather PII of Representative Plaintiffs and Class Members, misuse the PII and intentionally disclose it to others without consent.

e. by failing to adequately train their employees to not store PII longer than absolutely necessary;

f. by failing to consistently enforce security policies aimed at protecting Representative Plaintiffs' and the Class Members' PII;

g. by failing to implement processes to quickly detect data breaches, security incidents or intrusions; and

h. by failing to encrypt Representative Plaintiffs' and Class Members' PII and monitor user behavior and activity in order to identify possible threats.

127. Defendant's willful failure to abide by these duties was wrongful, reckless and grossly negligent in light of the foreseeable risks and known threats.

128. As a proximate and foreseeable result of Defendant's grossly negligent conduct, Representative Plaintiffs and Class Members have suffered damages and are at imminent risk of additional harms and damages.

129. The law further imposes an affirmative duty on Defendant to timely disclose the unauthorized access and theft of the PII to Representative Plaintiffs and Class Members so that they could and/or still can take appropriate measures to mitigate damages, protect against adverse consequences and thwart future misuse of its PII.

130. Defendant breached its duty to notify Representative Plaintiffs and Class Members of the unauthorized access by waiting months after learning of the Data Breach to notify

Representative Plaintiffs and Class Members and then by failing and continuing to fail to provide Representative Plaintiffs and Class Members sufficient information regarding the breach. To date, Defendant has not provided sufficient information to Representative Plaintiffs and Class Members regarding the extent of the unauthorized access and continues to breach its disclosure obligations to Representative Plaintiffs and Class Members.

131. Further, through its failure to provide timely and clear notification of the Data Breach to Representative Plaintiffs and Class Members, Defendant prevented Representative Plaintiffs and Class Members from taking meaningful, proactive steps to secure their PII.

132. There is a causal connection between Defendant's failure to implement security measures to protect the PII of Representative Plaintiffs and Class Members and the harm suffered or risk of imminent harm suffered by Representative Plaintiffs and Class Members. Representative Plaintiffs' and Class Members' PII was accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII by adopting, implementing and maintaining appropriate security measures.

133. Defendant's wrongful actions, inactions and omissions constituted common law negligence.

134. The damages Representative Plaintiffs and Class Members have suffered and will continue to suffer were and are the direct and proximate result of Defendant's grossly negligent conduct.

135. Additionally, 15 U.S.C. §45 (FTC Act, Section 5) prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect PII. The

FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

136. Defendant violated 15 U.S.C. § 45 by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII they obtained and stored and the foreseeable consequences of the immense damages that would result to Representative Plaintiffs and Class Members.

137. Defendant systematically failed to provide adequate security for data in its possession.

138. Defendant, 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' PII within its possession.

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

140. Defendant, through their actions and/or omissions, unlawfully breached its duty to timely disclose to Plaintiffs and Class Members that the PII within its possession might have been compromised and precisely the type of information compromised.

141. Defendant's breach of duties owed to Plaintiffs and Class Members caused Plaintiffs' and Class Members' PII to be compromised.

142. As a direct and proximate result of Defendant's negligence, Representative Plaintiffs and Class Members have suffered and will continue to suffer injury, including but not

limited to:

a. actual identity theft;

b. the loss of the opportunity of how their PII is used;

c. the compromise, publication and/or theft of their PII;

d. out-of-pocket expenses associated with the prevention, detection and recovery from identity theft, tax fraud and/or unauthorized use of their PII;

e. 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 embarrassment and identity theft;

f. the continued risk to their PII, which may remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Representative Plaintiffs' and Class Members' PII in their continued possession; and

g. future costs in terms of time, effort and money that will be expended to prevent, detect, contest and repair the impact of the compromised as a result of the Data Breach for the remainder of the lives of Representative Plaintiffs and Class Members.

143. As a direct and proximate result of Defendant's negligence, Representative Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including but not limited to anxiety, emotional distress, loss of privacy and other economic and non-economic losses.

144. Additionally, as a direct and proximate result of Defendant's negligence, Representative Plaintiffs and Class Members have suffered and will continue to suffer the continued risks of exposure of their PII, which remain in Defendant's possession and are subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

SECOND CLAIM FOR RELIEF
Breach of the Implied Contract
(On Behalf of Plaintiffs and the Class)

145. The allegations of the preceding paragraphs 1 through 114 are incorporated in this Cause of Action with the same force and effect as though fully set forth herein.

146. Representative Plaintiffs and Class Members were required to provide their PII to Defendant as a condition of obtaining employment at Defendant.

147. Representative Plaintiffs and the Class entrusted their PII to Defendant. In so doing, Representative Plaintiffs and the Class entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Representative Plaintiffs and the Class if their data had been breached and compromised or stolen.

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

149. Implicit in the agreement between Representative Plaintiffs and Class Members and the Defendant to provide PII, was the latter's obligation to: (a) use such PII for business purposes only, (b) take reasonable steps to safeguard that PII, (c) prevent unauthorized disclosures of the PII, (d) provide Representative Plaintiffs and Class Members with prompt

and sufficient notice of any and all unauthorized access and/or theft of their PII, (e) reasonably safeguard and protect the PII of Representative Plaintiffs and Class Members from unauthorized disclosure or uses, (f) retain the PII only under conditions that kept such information secure and confidential.

150. The mutual understanding and intent of Representative Plaintiffs and Class Members on the one hand, and Defendant, on the other, is demonstrated by their conduct and course of dealing.

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

152. In accepting the PII of Representative Plaintiffs and Class Members, Defendant understood and agreed that it was required to reasonably safeguard the PII from unauthorized access or disclosure.

153. On information and belief, at all relevant times Defendant promulgated, adopted, and implemented written privacy policies whereby it expressly promised Representative Plaintiffs and Class Members that it would only disclose PII under certain circumstances, none of which relate to the Data Breach.

154. On information and belief, Defendant further promised to comply with industry standards and to make sure that Representative Plaintiffs' and Class Members' PII would remain protected.

155. Representative Plaintiffs and Class Members provided their labor and PII to Defendant with the reasonable belief and expectation that Defendant would use part of its

earnings to obtain adequate data security. Defendant failed to do so.

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

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

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

159. Defendant breached the implied contracts it made with Representative Plaintiffs and the Class by failing to safeguard and protect their personal information, by failing to delete the information of Representative Plaintiffs and the Class once the relationship ended, and by failing to provide accurate notice to them that personal information was compromised as a result of the Data Breach.

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

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

162. Representative Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to, *e.g.*, (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii)

immediately provide adequate credit monitoring to all Class Members.

THIRD CLAIM FOR RELIEF
Unjust Enrichment
(On Behalf of Plaintiffs and the Class)

163. The allegations of the preceding paragraphs 1 through 114 are incorporated in this Cause of Action with the same force and effect as though fully set forth herein.

164. This count is brought in the alternative to the breach of implied contract claim above.

165. As an employee of Defendant, Plaintiffs provided Defendant with their PII.

166. In exchange, as an employee of Defendant, Plaintiffs and those similarly situated should have received adequate protection of their PII from Defendant.

167. Defendant knew that Plaintiffs and those similarly situated conferred a benefit which Defendant accepted. Defendant used the PII of Plaintiffs and those similarly situated for business purposes.

168. Specifically, Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' PII. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to increase its own profits at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite data security.

169. Under the principles of equity and good conscience, Defendant should not be permitted to retain a benefit belonging to Plaintiffs and those similarly situated because Defendant failed to implement appropriate data management and security measures that are mandated by

industry standards.

170. Defendant failed to secure Plaintiffs' and those similarly situated PII and, therefore, did not provide full compensation for the benefit Plaintiffs and those similarly situated provided.

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

172. Had Plaintiffs and those similarly situated known that Defendant had not reasonably secured their PII, they would not have agreed to do business with Defendant.

173. As a direct and proximate result of Defendant's conduct, Plaintiffs and those similarly situated have suffered and will suffer injury as set forth herein.

FOURTH CLAIM FOR RELIEF
Declaratory Judgment
(On Behalf of Plaintiffs and the Class)

174. The allegations of the preceding paragraphs 1 through 114 are incorporated in this Cause of Action with the same force and effect as though fully set forth herein. .

175. 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 grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

176. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiff's and Class Members' PII and whether Defendant is currently maintaining data security measures adequate to protect Plaintiffs and Class Members from further data breaches that compromise their PII. Plaintiffs allege that Defendant's data security measures remain inadequate, Furthermore, Plaintiffs continues to suffer injury as a result of the compromise of his PII and remains at imminent risk that further compromises of his PII will occur in the future.

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

a. Defendant owes a legal duty to secure employees' PII and to timely notify employees of a data breach under the common law, Section 5 of the FTC Act, and various state statutes; and

b. Defendant continues to breach this legal duty by failing to employ reasonable measures to secure employees' PII.

178. This Court also should issue corresponding prospective injunctive relief requiring Defendant to employ adequate security protocols consistent with law and industry standards to protect employees' PII.

179. If an injunction is not issued, Plaintiffs will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Defendant. The risk of another such breach is real, immediate, and substantial. If another breach at Defendant occurs, Plaintiffs will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and he will be forced to bring multiple lawsuits to rectify the same conduct.

180. The hardship to Plaintiffs if an injunction is not issued exceeds the hardship to Defendant if an injunction is issued. Plaintiffs will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to Defendant of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

181. Issuance of the requested injunction will not disserve the public interest. In contrast, such an injunction would benefit the public by preventing another data breach at Defendant, thus

eliminating the additional injuries that would result to Plaintiffs and employees whose confidential information would be further compromised.

RELIEF SOUGHT

WHEREFORE, Representative Plaintiffs, on behalf of themselves and each member of the proposed Class, respectfully request that the Court enter judgment in their favor and for the following specific relief against Defendant as follows:

1. That the Court declare, adjudge and decree that this action is a proper class action and certify the proposed Class under F.R.C.P. Rule 23 (b)(1), (b)(2), and/or (b)(3), including appointment of Representative Plaintiffs' counsel as Class Counsel;

2. For an award of damages including actual, nominal and consequential damages, as allowed by law in an amount to be determined;

3. That the Court enjoin Defendant, ordering it to cease and desist from unlawful activities;

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

5. For injunctive relief requested by Representative Plaintiffs, including but not limited to injunctive and other equitable relief as is necessary to protect the interests of Representative Plaintiffs and Class Members including but not limited to an Order:

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

   b. requiring Defendant to protect, including through encryption, all data

collected through the course of business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

c. requiring Defendant to delete and purge the PII of Representative Plaintiffs and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Representative Plaintiffs and Class Members;

d. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of Representative Plaintiffs' and Class Members' PII;

e. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring, simulated attacks, penetration tests and audits on Defendant's systems on a periodic basis;

f. prohibiting Defendant from maintaining Representative Plaintiffs' and Class Members' PII on a cloud-based database;

g. requiring Defendant to segment data by 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.

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

i. 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

Representative Plaintiffs and Class Members;

j. 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 personal identifying information:

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

l. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves.

6. For prejudgment interest on all amounts awarded at the prevailing legal rate;

7. For an award of attorneys' fees, costs and litigation expenses, as allowed by law;

8. For all other Orders, findings and determinations identified and sought in this Complaint.

JURY DEMAND

Representative Plaintiffs, individually, and on behalf of the Class hereby demand a trial by jury for all issues triable by jury.

DATED: February 26, 2024

Respectfully submitted,

/s/ Joe Kendall
JOE KENDALL
Texas Bar No. 11260700
SDTX Bar No. 30973
KENDALL LAW GROUP, PLLC
3811 Turtle Creek Blvd., Suite 825
Dallas, Texas 75219
Telephone: 214/744-3000 / 214/744-3015 (fax)
jkendall@kendalllawgroup.com

Gary Klinger (admitted *pro hac vice)*
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
227 W. Monroe Street
Suite 2100
Chicago, IL 60606
866-252-0878
gklinger@milberg.com

Brandon M. Wise*
PEIFFER WOLF CARR KANE CONWAY & WISE, LLP
818 Lafayette Ave., Floor 2
St. Louis, MO 63104
314-833-4825
bwise@peifferwolf.com

Daniel Srourian (admitted *pro hac vice)*
SROURIAN LAW FIRM, P.C.
3435 Wilshire Blvd., Suite 1710
Los Angeles, CA 90010
Telephone: (213) 474-3800
daniel@slfla.com

John A. Yanchunis
Ryan D. Maxey
MORGAN & MORGAN COMPLEX BUSINESS DIVISION
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
(813) 223-5505
jayanchunis@ForThePeople.com
rmaxey@ForThePeople.com

William B. Federman,
S.D. Tex. Bar No. 21540
FEDERMAN & SHERWOOD
10205 N. Pennsylvania Ave.
Oklahoma City, OK 73120
P: (405) 235-1560 F: (405) 239-2112
wbf@federmanlaw.com

Gary F. Lynch*
LYNCH CARPENTER LLP
1133 Penn Ave., 5th Floor
Pittsburgh PA, 15222
P: (412) 322-9243
gary@lcllp.com

Jeremy McDonald*
Chandler & McDonald, PLLC
101 N. McDowell St., Suite 210
Charlotte, North Carolina 28204
Telephone: (704) 376-6552
Fax: (704) 372-2003
Jmcdonald@charlottelawoffice.com

Theodore H. Huge*
Harris & Huge, LLC
180 Spring Street
Charleston, SC 29403
Telephone: (843) 805-8031
Fax: (843) 636-3375
ted@harrisandhuge.com

Attorneys for Plaintiffs and Putative Class
**pro hac vice application forthcoming*

CERTIFICATE OF SERVICE

I hereby certify that a copy of the foregoing document was served on all counsel of record on February 26, 2024 via CM/ECF, in accordance with the Federal Rules of Civil Procedure.

/s/ *Joe Kendall*
JOE KENDALL