IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO
EASTERN DIVISION

JOHN DOE, on behalf of himself and all others similarly situated, Plaintiff, v. THE MISSION ESSENTIAL GROUP, LLC, Defendant.	Case No. **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff, John Doe, through his attorneys, brings this Class Action Complaint against the Defendant, The Mission Essential Group, LLC ("MEG" or "Defendant"), alleging as follows:

INTRODUCTION

1. In September 2022, MEG, a government contractor providing valuable and sensitive translation services and solutions to global threats, terrorism, and risks to American security, lost control over its computer network and the highly sensitive private information stored on the computer network in a data breach perpetrated by cybercriminals ("Data Breach"). The number of total breach victims is unknown, but on information and belief, the Data Breach has impacted at least thousands of former and current employees.

2. MEG has disclosed that it was informed by federal law enforcement authorities about the Data Breach in September 2022. *See* Ex. A at 1. Due to MEG's intentionally obfuscating language, little is known about how and when cybercriminals gained unfettered access to Defendant's network.

3. On April 19, 2023, following an internal investigation, Defendant learned

cybercriminals potentially gained unauthorized access to former and current employees' personally identifiable information ("PII"). However, on information and belief, Defendant's cyber and data security systems and measures were so inadequate that Defendant was unable to identify when and how the Data Breach identified by federal law enforcement authorities occurred.

4. On July 20, 2023, MEG finally notified Class Members about the widespread Data Breach ("Breach Notice"). Plaintiff's Breach Notice has been attached as **Exhibit A**, with his name and address redacted. Defendant waited an appalling ten months before informing Class Members, even though Plaintiff and the Class had their most sensitive personal information accessed, exfiltrated, and stolen, causing them to not only suffer ascertainable losses in the form of the loss of the benefit of their bargain and the value of their time reasonably incurred to remedy or mitigate the effects of the attack, but also imminent threat of physical danger by hostile government actors and terrorists due to the geopolitically sensitive work Plaintiff and Class Members performed.

5. Defendant's Breach Notice obfuscated the nature of the breach and the threat it posted—refusing to tell its victims how many people were impacted, why it required federal law enforcement authorities to alert Defendant about the Breach, or why it took the Defendant ten months to begin notifying some of its victims that hackers had gained access to highly sensitive PII.

6. Defendant's failure to timely detect and report the Data Breach made its employees vulnerable to imminent physical danger, without any warnings about how the Data Breach renders them sitting ducks for identification, capture and interrogation by terrorists and hostile government actors, particularly if they leave American soil.

7. Defendant's failures also made its employees vulnerable to identity theft, without any warnings to Plaintiff and the Class to monitor their financial accounts and credit reports to

prevent unauthorized use of their PII.

8. Defendant knew or should have known that each victim of the Data Breach deserved prompt and efficient notice of the Data Breach and assistance in mitigating the effects of PII misuse.

9. In failing to adequately protect employees' information, adequately notify them about the breach, and obfuscating the nature of the breach, Defendant violated state law and harmed an unknown number of its former and current employees.

10. Plaintiff and members of the proposed Class are victims of Defendant's negligence and inadequate cyber security measures. Specifically, Plaintiff and the Class trusted Defendant with their PII. But Defendant betrayed that trust. Defendant failed to properly use up-to-date security practices to prevent the Data Breach.

11. Plaintiff is a former MEG employee and a Data Breach victim.

12. The exposure of one's PII to cybercriminals is a bell that cannot be unrung. Before this data breach, victims' private information was exactly that—private. Not anymore. Now, Plaintiff's and the Class's private information is forever exposed and unsecure, rendering them vulnerable to identity theft, fraud, and physical harm.

PARTIES

13. Plaintiff, John Doe, is a natural person and citizen of Georgia, where he intends to remain. Mr. Doe is a Data Breach victim, and received MEG's Breach Notice on July 25, 2023.

14. Defendant, The Mission Essential Group, LLC, is an Ohio limited liability company with its principal place of business at 6525 W Campus Oval, Ste 101, New Albany, Ohio, 43054.

JURISDICTION & VENUE

15. This Court has subject matter jurisdiction over this action under 28 U.S.C.§ 1332(d)

because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class. Defendant and Plaintiff are citizens of different states.

16. This Court has personal jurisdiction over Defendant because Defendant maintains its principal place of business in this District and does substantial business in this District.

17. Venue is proper in this District under 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to the claim occurred in this District.

BACKGROUND FACTS

MEG

18. MEG prides itself as "an agile, trusted partner, [providing translators and interpreters] to the Defense and Intelligence communities, friendly foreign governments, and select private sector segments."[1] MEG boasts an annual revenue of $500 million.[2]

19. MEG specializes in supporting "intelligence operations for warfighters" by providing "difficult-to-find language experts in the Middle East, Africa, and Asia" that reveal "relevant intelligence about the activities, capabilities, plans, and intentions of potential threats, both home and abroad, to inform decisions on national security issues and events." Through these polyglot language experts, MEG helps "protect and defend [customers like the Department of Defense'] interests against terrorism [] and other hazards to global security."[3]

20. On information and belief, Defendant receives and maintains the PII of thousands of former and current employees, for years after the employee's relationship with Defendant is

[1] MEG, About, https://www.missionessential.com/company/#:~:text=The%20Mission%20Essential%20Group%20is,and%20select%20private%20sector%20segments (last visited September 28, 2023).
[2] Zippia, MEG Revenue, https://www.zippia.com/mission-essential-careers-31636/revenue/ (last visited September 28, 2023).
[3] Capabilities, MEG, https://www.missionessential.com/capabilities-2/ (last visited October 7, 2023).

terminated.

21. MEG promises in its privacy policy that it is "committed to safeguarding your privacy."[4] MEG's need for safeguarding its employees' privacy is particularly important given the extremely sensitive geopolitical work its employees perform on its behalf.

22. MEG further assures its employees that it "uses administrative, technical, and physical security measures to protect your personal information. These measures include following stringent procedures, ensuring the maintenance of our physical and electronic security safeguards, and strictly adhering to our data protection policies."[5]

23. In collecting and maintaining consumers' PII, MEG 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.

24. Despite recognizing its duty to do so, on information and belief, MEG has not in fact implemented reasonably cybersecurity safeguards or policies to protect its employees' PII or trained its IT or data security employees to prevent, detect, and stop breaches of its systems. As a result, MEG leaves significant vulnerabilities in its systems for cybercriminals to exploit and gain access to former and current employees' PII.

MEG Fails to Safeguard Employees' PII

25. Plaintiff is a former employee of MEG.

26. As a condition of employment with MEG, Defendant requires its employees to disclose PII including but not limited to, their name and Social Security number. 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.

[4] MEG, Privacy Policy, https://www.missionessential.com/privacy-policy-2/ (last visited September 28, 2023).
[5] *Id.*

27. On information and belief, MEG collects and maintains current and former employees' PII in its computer systems.

28. In collecting and maintaining the PII, MEG implicitly agrees it will safeguard the data using reasonable means according to its internal policies and federal law.

29. According to the Breach Notice, MEG claims to have been "notified by federal law enforcement authorities of a potential incident wherein certain Mission Essential email accounts may have been accessed and/or acquired by an unauthorized actor" in September 2022. Following an internal investigation, MEG admitted that "the types of information potentially present in Mission Essential email accounts may relate to Mission Essential current and former employees or contractors, or those individual's spouses, dependents, or beneficiaries and include Social Security number, and name." Ex. A.

30. So inadequate were Defendant's cyber and data security systems and measures, that Defendant admitted it was unable to identify when the Data Breach occurred, how its network was hacked, and if it was cybercriminals, terrorists, or hostile government actors that perpetrated the hack. Further, Defendant intentionally obfuscated the circumstances surrounding how the federal law enforcement authorities discovered MEG's breach. Ex. A.

31. Through its inadequate security practices, Defendant not only exposed Plaintiff's and the Class's PII for theft and sale on the dark web, but also exposed Plaintiff and the Class to imminent physical danger from hostile government actors and terrorists due to the highly valuable and sensitive geo-political translation work they performed as "difficult-to-find language experts." [6]

32. On or about July 20, 2023 – ten months after federal law enforcements authorities

[6] Capabilities, MEG, https://www.missionessential.com/capabilities-2/ (last visited October 7, 2023).

first alerted MEG to the Breach – MEG finally notified Plaintiff and Class Members about the Data Breach.

33. Despite its duties and alleged commitments to safeguard PII, MEG does not follow industry standard practices in securing former and current employees' PII, as evidenced by the Data Breach.

34. In response to the Data Breach, MEG contends that it has or will be "reviewing and updating existing policies and procedures relating to data protection and security" Ex. A. Although MEG fails to expand on what these alleged "updates" to policies and procedures are, such updates should have been in place before the Data Breach.

35. Through its Breach Notice, MEG also recognized the actual imminent harm and injury that flowed from the Data Breach, so it encouraged breach victims "remain vigilant against incidents of identity theft and fraud." Ex. A.

36. MEG further recognized through its Breach Notice, its duty to implement reasonable cybersecurity safeguards or policies to protect its employees' PII, promising that, despite having to have federal law enforcement authorities alert it of a breach, "Mission Essential treats its responsibility to safeguard information in its care as an utmost priority" Ex. A.

37. On information and belief, MEG has offered a year of complimentary credit monitoring services to victims, which does not adequately address the lifelong harm that victims will face following the Data Breach. Indeed, the breach involves PII that cannot be changed, such as Social Security numbers. Furthermore, a year of complimentary credit monitoring does nothing to address the lifelong risk of physical harm the victims now face as targets of hostile government actors and terrorists.

38. Additionally, even with a year of credit monitoring services, the risk of identity

theft and unauthorized use of Plaintiff's and Class Members' PII is still substantially high. The fraudulent activity resulting from the Data Breach may not come to light for years.

39. Cybercriminals need not harvest a person's Social Security number or financial account information in order to commit identity fraud or misuse Plaintiff's and the Class's PII. Cybercriminals can cross-reference the data stolen from the Data Breach and combine with other sources to create "Fullz" packages, which can then be used to commit fraudulent account activity on Plaintiff's and the Class's financial accounts.

40. Cybercriminals need not harvest a person's Social Security number or financial account information in order to commit identity fraud or misuse Plaintiff's and the Class's PII. Cybercriminals can cross-reference the data stolen from the Data Breach and combine this with other sources to create "Fullz" packages, which can then be used to commit fraudulent account activity on Plaintiff's and the Class's financial accounts.

41. On information and belief, MEG failed to adequately train its IT and data security employees on reasonable cybersecurity protocols or implement reasonable security measures, causing it to lose control over its former and current employees' PII. Defendant's negligence is evidenced by its failure to prevent the Data Breach and stop cybercriminals from accessing the PII.

Plaintiff's Experience

42. Plaintiff John Doe is a former MEG employee.

43. Plaintiff is fluent in multiple "difficult-to-find" languages of interest to the United States Government and worked for the U. S. Government following the September 11 attacks. Like other Class Members, Plaintiff John Doe was hired by MEG for his polyglot skills and experience in highly sensitive geopolitical relations and translation work.

44. As a condition of employment with MEG, Plaintiff was required to provide his PII,

including but not limited to his full name and Social Security number.

45. Plaintiff provided his PII to MEG and trusted that the company would use reasonable measures to protect it according to Defendant's internal policies, as well as state and federal law.

46. MEG deprived Plaintiff of the earliest opportunity to guard his PII against the Data Breach's effects by failing to notify him about it for over ten months.

47. Defendant exposed Plaintiff's PII for theft and sale by cybercriminals, hostile government actors, and terrorists, who are now able to identify Plaintiff through the PII lost by MEG, and gather additional information on Plaintiff, including photographs of Plaintiff. Defendant thereby compromised Plaintiff's safety and exposed him to imminent physical harm, including blackmail, capture and interrogation, and other forms of danger.

48. As a result of the Data Breach and the recommendation of Defendant's Notice, Mr. Doe has 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 and credit reports to ensure no fraudulent activity has occurred. This time has been lost forever and cannot be recaptured.

49. Mr. Doe has and will spend considerable time and effort monitoring his accounts to protect himself from identity theft and physical harm. Mr. Doe fears for his physical safety as well as his personal financial security and uncertainty over what PII exposed in the Data Breach. Mr. Doe has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

50. Plaintiff suffered actual injury from the exposure of his PII—which violates his rights to privacy.

51. Plaintiff has suffered actual injury in the form of damages to and diminution in the value of his PII—a form of intangible property that Plaintiff entrusted to Defendant, which was compromised in and as a result of the Data Breach.

52. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of physical danger, fraud, identity theft, and misuse resulting from his PII being placed in the hands of unauthorized third parties, including cybercriminals, hostile government actors, and terrorists.

53. Indeed, following the Data Breach, Plaintiff began receiving strange and concerning military-related emails, including fraudulent offers for a military translation job, that appear to be of Russian origin. Plaintiff has also begun receiving crypto currency links. Both forms of emails are sent from unfamiliar Gmail addresses that Plaintiff does not recognize. These emails suggest Plaintiff's PII has been placed in the hands of cybercriminals, hostile government actors, and terrorists.

54. 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 future breaches.

Plaintiff and the Proposed Class Face Significant Risk of Continued Identity Theft

55. Plaintiff and members of the proposed Class have suffered injury from the misuse of their PII that can be directly traced to Defendant.

56. 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, date of birth, Social Security number, or driver's license

number, without permission, to commit fraud or other crimes. Further, Plaintiff's and the Class's physical safety and security have been compromised as a result of Defendant's failure to keep their PII private.

57. The types of PII compromised and potentially stolen in the Data Breach is highly valuable to identity thieves. The employees' stolen PII can be used to gain access to a variety of existing accounts and websites to drain assets, bank accounts or open phony credit cards.

58. Social Security numbers are particularly attractive targets for hackers because they can easily be used to perpetrate identity theft and other highly profitable types of fraud. Moreover, Social Security numbers are difficult to replace, as victims are unable to obtain a new number until the damage is done.

59. Identity thieves can also use the stolen data to harm Plaintiff and Class members through embarrassment, blackmail, or harassment in person or online, or to commit other types of fraud including obtaining ID cards or driver's licenses, fraudulently obtaining tax returns and refunds, and obtaining government benefits. A Presidential Report on identity theft from 2008 states that:

> In addition to the losses that result when identity thieves fraudulently open accounts or misuse existing accounts, . . . individual victims often suffer indirect financial costs, including the costs incurred in both civil litigation initiated by creditors and in overcoming the many obstacles they face in obtaining or retaining credit. Victims of non-financial identity theft, for example, health- related or criminal record fraud, face other types of harm and frustration.
>
> In addition to out-of-pocket expenses that can reach thousands of dollars for the victims of new account identity theft, and the emotional toll identity theft can take, some victims have to spend what can be a considerable amount of time to repair the damage caused by the identity thieves. Victims of new account identity theft, for example, must correct fraudulent information in their credit reports and monitor their reports for future inaccuracies,

close existing bank accounts and open new ones, and dispute charges with individual creditors.

60. As a result of Defendant's failure to prevent the Data Breach, Plaintiff and the proposed Class have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at an increased risk of suffering:

a. The loss of the opportunity to control how their PII is used;

b. The diminution in value of their PII;

c. The compromise and continuing publication of their PII;

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

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

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen PII; and

h. 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.

61. 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.

62. The value of Plaintiff's and the proposed Class's PII on the black market is considerable. Stolen PII trades on the black market for years, and criminals frequently post stolen

private information openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

63. It can take victims years to spot identity or PII theft, giving criminals plenty of time to use that information for cash.

64. One such example of criminals using PII for profit is the development of "Fullz" packages.

65. Cyber-criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

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

67. Defendant disclosed the PII of Plaintiff and members of the proposed Class for criminals to use in the conduct of criminal activity. Specifically, Defendant opened up, disclosed, and exposed the PII of Plaintiff and members of the proposed Class to people engaged in disruptive

and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen PII. Further, Defendant opened up and exposed the PII of Plaintiff and the Class to terrorists and hostile government actors who are engaged in interests and tactics that threaten the physical safety of Plaintiff and the Class, including blackmail, threats, and the capture and extraction of highly valuable geopolitical information from Plaintiff and the Class.

68. Defendant's use of outdated and insecure computer systems and software that are easy to hack, and its failure to maintain adequate security measures and an up-to-date technology security strategy, as evidenced by its complete failure to prevent malware in its systems, demonstrates a willful and conscious disregard for privacy, and has exposed the PII of Plaintiff and the Class to unscrupulous operators, con-artists, hostile government actors, terrorists, and criminals.

69. Defendant's failure to properly notify Plaintiff and members of the proposed Class of the Data Breach exacerbated Plaintiff's and the Class's injuries by depriving them of the earliest ability to take appropriate measures to protect their PII and take other necessary steps to mitigate the harm caused by the Data Breach.

Defendant failed to adhere to FTC guidelines.

70. 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.

71. 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.

72. 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.

73. 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.

74. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer, or in this case, employees' 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.

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

Defendant Failed to Follow Industry Standards

76. Several best practices have been identified that—at a *minimum*—should be implemented by businesses like Defendant. These industry standards include: educating all

employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption (making data unreadable without a key); multi-factor authentication; backup data; and limiting which employees can access sensitive data.

77. Other industry standard best practices include: installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

78. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

79. These frameworks are applicable and accepted industry standards. And by failing to comply with these accepted standards, Defendant opened the door to the criminals—thereby causing the Data Breach.

CLASS ACTION ALLEGATIONS

80. Plaintiff brings this action pursuant to Federal Rule of Civil Procedure 23 on behalf of himself and all members of the proposes class (the "Class"), defined as follows:

> **All individuals in the United States whose PII was accessed without authorization in the Data Breach, including all those who received a notice of the Data Breach.**

81. Excluded from the Class is Defendant, its agents, affiliates, parents, subsidiaries, any entity in which Defendant has a controlling interest, any Defendant officer or director, any

successor or assign, and any Judge who adjudicates this case, including their staff and immediate family.

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

83. **Numerosity**. Plaintiff is representative of the proposed Class, consisting of several thousands of Class Members, far too many to join in a single action;

84. **Ascertainability**. Class members are readily identifiable from information in Defendant's possession, custody, and control;

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

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

87. **Commonality.** Plaintiff's and the Class's claims raise predominantly common fact and legal questions that a class wide proceeding can answer for all Class members. Indeed, it will be necessary to answer the following questions:

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

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

c. Whether Defendant was negligent in maintaining, protecting, and securing PII;

d. Whether Defendant breached contract promises to safeguard Plaintiff's and the Class's PII;

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

f. Whether Defendant's Breach Notice was reasonable;

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

h. What the proper damages measure is; and

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

88. Further, common questions of law and fact predominate over any individualized questions, and a class action is superior to individual litigation or any other available method to fairly and efficiently adjudicate the controversy. The damages available to individual plaintiffs are insufficient to make individual lawsuits economically feasible.

COUNT I
Negligence
(On Behalf of Plaintiff and the Class)

89. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

90. Plaintiff and members of the Class entrusted their PII to MEG. Defendant owed a duty to Plaintiff and the Class to exercise reasonable care in safeguarding and protecting their PII 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 PII of Plaintiff 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.

91. MEG was under a basic duty to act with reasonable care when it undertook to

collect, create, and store Plaintiff's and the Class's PII 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.

92. Defendant knew that the PII of Plaintiff and the Class was information that is valuable to identity thieves and other criminals. Defendant also knew of the serious harms that could happen if the PII of Plaintiff and the Class was wrongfully disclosed.

93. By being entrusted by Plaintiff and the Class to safeguard their PII, Defendant had a special relationship with Plaintiff and the Class. Plaintiff's and the Class's PII was provided to MEG 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.

94. Defendant breached its duty to exercise reasonable care in safeguarding and protecting Plaintiff's and the Class members' PII by failing to adopt, implement, and maintain adequate security measures to safeguard that information and allowing unauthorized access to Plaintiff's and the Class's PII.

95. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and the Class, their PII would not have been compromised, stolen, and viewed by unauthorized persons. Defendant's negligence was a direct and legal cause of the theft of the PII of Plaintiff and the Class and all resulting damages.

96. The injury and harm suffered by Plaintiff and the Class members was the reasonably foreseeable result of Defendant's failure to exercise reasonable care in safeguarding and protecting Plaintiff's and the Class members' PII.

97. As a result of Defendant's failure, the PII of Plaintiff and the Class were compromised, placing them at a greater risk of identity theft and subjecting them to identity theft, and their PII was disclosed to third parties without their consent. Plaintiff and Class members also suffered diminution in value of their PII in that it is now easily available to hackers on the Dark Web. Plaintiff and the Class have also suffered consequential out of pocket losses for procuring credit freeze or protection services, identity theft monitoring, and other expenses relating to identity theft losses or protective measures.

COUNT II
Negligence *Per Se*
(On Behalf of Plaintiff and the Class)

98. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

99. Pursuant to the FTC Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and members of the Class's PII.

100. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect consumers' PII. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiff's and the Class's sensitive PII.

101. Defendant violated its duty under Section 5 of the FTC Act 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 Defendant had collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

102. The harm that has occurred is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

103. Defendant had a duty to Plaintiff and the Class to implement and maintain reasonable security procedures and practices to safeguard Plaintiff's and the Class's PII.

104. Defendant breached its respective duties to Plaintiff and members of the Class under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and members of the Class's PII.

105. Defendant's violation of Section 5 of the FTC Act and its failure to comply with applicable laws and regulations constitutes negligence *per se*.

106. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and members of the Class, Plaintiff and the Class would not have been injured.

107. The injury and harm suffered by Plaintiff and the Class were the reasonably foreseeable result of Defendant's breach of their duties. Defendant knew or should have known that Defendant was failing to meet its duties and that its breach would cause Plaintiff and members of the Class to suffer the foreseeable harms associated with the exposure of their PII.

108. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and the Class have suffered harm, including loss of time and money resolving fraudulent charges; loss of

time and money obtaining protections against future identity theft; lost control over the value of PII; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen personal information, entitling them to damages in an amount to be proven at trial.

COUNT III
Breach of Implied Contract
(On Behalf of Plaintiff and the Class)

109. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

110. Plaintiff and Class Members were required to provide their PII Defendant as a condition of receiving employment from Defendant. Plaintiff and Class Members provided their PII to Defendant in exchange for Defendant's employment.

111. Plaintiff and Class Members reasonably understood that a portion of the funds from their employment would be used by Defendant to pay for adequate cybersecurity and protection of their PII.

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

113. In turn, and through internal policies, Defendant agreed to protect and not disclose the PII to unauthorized persons.

114. In its Privacy Policy, Defendant represented that they had a legal duty to protect Plaintiff's and Class Member's PII.

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

116. After all, Plaintiff and Class Members would not have entrusted their PII to

Defendant in the absence of such an agreement with Defendant.

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

118. The covenant of good faith and fair dealing is an element of every contract. Thus, 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—and not merely the letter—of the bargain. In short, the parties to a contract are mutually obligated to comply with the substance of their contract in addition to its form.

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

120. Defendant materially breached the contracts it entered with Plaintiff and Class Members by:

a. failing to safeguard their information;

b. failing to notify them promptly of the intrusion into its computer systems that compromised such information.

c. failing to comply with industry standards;

d. failing to comply with the legal obligations necessarily incorporated into the agreements; and

e. failing to ensure the confidentiality and integrity of the electronic PII that Defendant created, receive and maintained.

121. In these and other ways, Defendant violated its duty of good faith and fair dealing.

122. Defendant's material breaches were the direct and proximate cause of Plaintiff's and Class Members' injuries (as detailed *supra*).

COUNT IV
Breach of Fiduciary Duty
(On Behalf of Plaintiff and the Class)

123. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

124. Given the relationship between Defendant and Plaintiff and Class Members, where Defendant became guardian of Plaintiff and Class Members' PII, Defendant became a fiduciary by its undertaking and guardianship of the PII, to act primarily for Plaintiff and Class Members, (1) for the safeguarding of Plaintiff and Class Members' PII; (2) to timely notify Plaintiff and Class Members of a Data Breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendant did and does store.

125. Defendant has a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of Defendant's relationship with them—especially to secure their PII.

126. Because of the highly sensitive nature of the PII, Plaintiff and Class Members would not have entrusted Defendant, or anyone in Defendant's position, to retain their PII had they known the reality of Defendant's inadequate data security practices.

127. Defendant breached its fiduciary duties to Plaintiff and Class Members by failing to sufficiently encrypt or otherwise protect Plaintiff and Class Members' PII.

128. Defendant also breached its fiduciary duties to Plaintiff and Class Members by failing to diligently discover, investigate, and give notice of the Data Breach in a reasonable and practicable period.

129. As a direct and proximate result of Defendant's breach of its fiduciary duties,

Plaintiff and Class Members have suffered and will continue to suffer numerous injuries (as detailed *supra*).

COUNT V
Invasion of Privacy/Intrusion upon Seclusion
(On Behalf of Plaintiff and the Class)

130. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

131. Ohio recognizes the tort of Invasion of Privacy— the wrongful intrusion into one's private activities in such a manner as to outrage or cause mental suffering, shame, or humiliation to a person of ordinary sensibilities.

132. Plaintiff and the Class had a legitimate expectation of privacy regarding their highly sensitive and confidential PII and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

133. Defendant owed a duty to its employees, including Plaintiff and the Class, to keep this information confidential.

134. The unauthorized acquisition (i.e., theft) by a third party of Plaintiff's and Class Members' PII is highly offensive to a reasonable person.

135. The intrusion was into a place or thing which was private and entitled to be private. Plaintiff and the Class disclosed their sensitive and confidential information to Defendant, but did so privately, with the intention that their information would be kept confidential and protected from unauthorized disclosure. Plaintiff and the Class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

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

137. Defendant acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

138. Defendant acted with a knowing state of mind when it failed to notify Plaintiff and the Class in a timely fashion about the Data Breach, thereby materially impairing their mitigation efforts.

139. Acting with knowledge, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiff and the Class.

140. As a proximate result of Defendant's acts and omissions, the private and sensitive PII of Plaintiff and the Class were stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiff and the Class to suffer damages (as detailed supra).

141. Unless and until enjoined and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Class since their PII are still maintained by Defendant with their inadequate cybersecurity system and policies.

142. Plaintiff and the Class have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential records. A judgment for monetary damages will not end Defendant's inability to safeguard the PII of Plaintiff and the Class.

143. In addition to injunctive relief, Plaintiff, on behalf of himself and the other Class Members, also seeks compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest and costs.

COUNT VI
Unjust Enrichment

(On Behalf of Plaintiff and the Class)

144. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

145. This claim is pleaded in the alternative to the breach of contract claim.

146. Plaintiff and Class Members conferred a benefit upon Defendant. After all, Defendant benefitted from using their PII to facilitate its business.

147. Defendant appreciated or had knowledge of the benefits it received from Plaintiff and Class Members. And Defendant benefited from receiving Plaintiff's and Class Members' PII, as this was used to provide suits business.

148. Plaintiff and Class Members reasonably understood that Defendant would use adequate cybersecurity measures to protect the PII that they were required to provide based on Defendant's duties under state and federal law and its internal policies.

149. Defendant enriched itself by saving the costs they reasonably should have expended on data security measures to secure Plaintiff's and Class Members' PII.

150. Instead of providing a reasonable level of security, or retention policies, that would have prevented the Data Breach, Defendant instead calculated to avoid its data security obligations 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 failure to provide the requisite security.

151. Under principals of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiff and Class Members' payments because Defendant failed to adequately protect their PII.

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

153. Defendant should be compelled to disgorge into a common fund—for the benefit

of Plaintiff and Class Members—all unlawful or inequitable proceeds that it received because of its misconduct.

PRAYER FOR RELIEF

154. Plaintiff and members of the Class demand a jury trial on all claims so triable and request 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. Awarding declaratory and other equitable relief as is necessary to protect the interests of Plaintiff and the Class;

C. Awarding injunctive relief as is necessary to protect the interests of Plaintiff and the Class;

D. Enjoining Defendant from further deceptive practices and making untrue statements about the Data Breach and the stolen PII;

E. Awarding Plaintiff and the Class damages that include applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;

F. Awarding restitution and damages to Plaintiff and the Class in an amount to be determined at trial;

G. Awarding attorneys' fees and costs, as allowed by law;

H. Awarding prejudgment and post-judgment interest, as provided by law;

I. Granting Plaintiff and the Class leave to amend this complaint to conform to the evidence produced at trial; and

J. Granting such other or further relief as may be appropriate under the

circumstances.

JURY DEMAND

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

DATED: October 11, 2023

Respectfully submitted,

/s/ Terence R. Coates
Terence R. Coates (0085579) – Trial Attorney
MARKOVITS, STOCK & DEMARCO, LLC
119 East Court Street, Suite 530
Cincinnati, OH 45202
Telephone: (513) 651-3700
Fax: (513) 665-0219
tcoates@msdlegal.com

Samuel J. Strauss *
sam@turkestrauss.com
Raina C. Borrelli *
raina@turkestrauss.com
TURKE & STRAUSS LLP
613 Williamson St., Suite 201
Madison, WI 53703
Telephone (608) 237-1775
Facsimile: (608) 509-4423

Attorneys for Plaintiff and the Proposed Class

* *Motions for admission* pro hac vice *forthcoming*