MEYER WILSON CO., LPA
Matthew R. Wilson (SBN 290473)
mwilson@meyerwilson.com
Michael J. Boyle, Jr. (SBN 258560)
mboyle@meyerwilson.com
Jared W. Connors (*pro hac vice* to be filed)
jconnors@meyerwilson.com
305 W. Nationwide Blvd.
Columbus, OH 43215
Telephone: (614) 224-6000
Facsimile: (614) 224-6066

TURKE & STRAUSS LLP
Raina Borrelli (*pro hac vice* to be filed)
raina@turkestrauss.com
613 Williamson St., #201
Madison, WI 53703
P: (608) 237-1775

Attorneys for Plaintiff and the Proposed Class

IN THE DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

MADELEINE BRASCH, on behalf of herself and all others similarly situated,

Plaintiff,

v.

MEYER CORPORATION, U.S.

Defendant.

Case No. 4:22-cv-03570

Class Action Complaint

Plaintiff Madeleine Brasch, through her attorneys, brings this Class Action Complaint against the Defendant, Meyer Corporation, U.S. ("Meyer" or "Defendant"), alleging as follows:

INTRODUCTION

1. In October 2021, Meyer, a cookware manufacturing company employing thousands of employees, lost control over at least 2,747 employees' highly sensitive personal information in a data breach ("Data Breach"), and then failed to notify its employees about the breach for nearly four months while cybercriminals publicly claimed responsibility for the Data Breach and published certain stolen data to prove what they had done.

2. Cybercriminals bypassed Meyer's inadequate security systems using ransomware to access employees' personally identifiable information ("PII"), including their names, addresses, dates of birth, gender and race information, Social Security numbers, driver's license numbers, and

medical information—including, but not limited to—medical conditions, prior drug tests, and COVID vaccination cards and statuses. The cybercriminals also accessed information regarding the employees' immigration statuses and their dependents' PII.

3. On or around October 25, 2021, cybercriminals breached Meyer's systems and impacted its operations. It is unknown for how long the breach went undetected before Meyer detected it, meaning Meyer had no effective means to prevent, detect, or stop the Data Breach from happening before cybercriminals stole and misused employees' PII. On or around December 1, 2021, Meyer's investigation confirmed the unauthorized access to its employees' PII. Instead of alerting its employees immediately, as required under California law, Meyer hid the breach from current and former employees until February 2022, even after cybercriminals posted a percentage of the leaked data online.

4. On February 15, 2022, Meyer finally informed its current and former employees of the Data Breach and offered them 24 months of free credit monitoring service, which fails to adequately address the lifelong threat the Data Breach poses to impacted employees.

5. Meyer's failures to adequately protect employee PII and timely notify employees about the devastating Data Breach harms its current and former employees in violation of California law.

6. Plaintiff Brasch is a former Meyer employee and Data Breach victim. She brings this action on behalf of herself and all others harmed by Meyer's misconduct, seeking relief on a class wide basis.

PARTIES

7. Plaintiff Madeleine Brasch is a natural person and citizen of California residing in Hayward, California, where she intends to remain. Plaintiff Brasch is a former Meyer employee and Data Breach victim, which Meyer confirmed to her when she called the data breach hotline at 888-292-0076.

8. Defendant Meyer Corp. is a Delaware corporation registered to do business in California, with its principal place of business at 525 Curtola Parkway, Vallejo, CA 94590.

JURISDICTION & VENUE

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

because at least one member of the proposed Class is a citizen of a state different from that of Meyer;[1] the amount in controversy exceeds $5,000,000, exclusive of interest and costs; the proposed Class consists of more than 100 class members, and none of the exceptions under the subsection apply to this action.

10. This Court has personal jurisdiction over Defendant because Meyer is registered to do business in California and is subject to this Court's general and specific jurisdiction given that it is headquartered in California and that this cause of action arises out of events that took place in California.

11. Venue is proper 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this district—namely, she suffered severe mental and emotional distress at her place of residence located in Alameda County.

BACKGROUND FACTS

a. Meyer

12. Meyer describes itself as "The global innovator of the highest quality brands of cookware and bakeware in the world[,]" with over 3,500 employees.[2] Meyer conducts its business internationally and owns a significant portfolio of other kitchenware brands.[3]

13. Meyer does and has employed thousands of individuals, with the Data Breach impacting over 2,700 current and former employees.

14. Meyer requires that its employees disclose their PII as part of their employment with Meyer, including their names, income information, Social Security numbers, driver's license numbers, medical information, and financial account numbers.

15. As a large employer managing employees' highly sensitive PII, Meyer understands its

---

[1] *See, e.g.*, *Reported Data Breach Incidents*, MONTANA DEPT. OF JUSTICE (accessed June 16, 2022), https://dojmt.gov/consumer/databreach (reporting that four Montana residents were affected by Meyer's data breach).

[2] *See* Meyer's website, https://meyerus.com/about/ (last visited Mar. 23, 2022).

[3] *See* Meyer's website, http://meyerus.com/brands/ (last visited Mar. 23, 2022).

duty to safeguard employee PII using reasonable means, informing employees that "The security of [their] information is a top priority, and [Meyer is] committed to the protection of [the employees'] information."[4]

16. Despite recognizing its duty to do so Meyer has not implemented reasonable cybersecurity safeguards or policies to protect current and former employee PII, or trained its employees to prevent, detect, and stop data breaches of Meyer's systems. As a result, Meyer leaves vulnerabilities in its systems for cybercriminals to exploit and give access to employee PII.

17. Indeed, upon investigation of counsel, Meyer has previously been subject to other data breaches. Meyer has therefore displayed a pattern of institutional failure to safeguard highly sensitive employee information.

b. Meyer Fails to Safeguard Employee PII

18. Meyer requires its employees to disclose their PII as a condition of employment at Meyer.

19. Meyer collects and maintains employee PII in its computer systems.

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

21. Despite its duties to safeguard employee PII, on October 25, 2021, cybercriminals bypassed Meyer's security systems undetected and accessed employee information.

22. On or around December 1, 2021, Meyer finally discovered that cybercriminals accessed employee PII, saying that it "identified potential unauthorized access to employee information,"[5] though Meyer has never disclosed the exact date it became aware of the Data Breach.

23. Despite the devastating nature of the breach, Meyer did not immediately inform its

---

[4] *See* Meyer's sample breach notice provided to the office of California's Attorney General, https://oag.ca.gov/system/files/MCorp%20U.S.%20Sample%20Letters.pdf (last visited Mar. 23, 2022).

[5] *See* Meyer's sample breach notice provided to the office of California's Attorney General, https://oag.ca.gov/system/files/MCorp%20U.S.%20Sample%20Letters.pdf (last visited Mar. 23, 2022).

employees about the breach or otherwise notify them according to California law. Instead, Meyer initiated an internal investigation with its "cybersecurity experts."[6]

24. On information and belief, a cybercriminal group known as the "Conti Ransomware Group" publicly claimed responsibility for the Data Breach on or around November 7, 2021. The Conti cybercriminals published at least 2% of the stolen data online.[7]

25. On February 15, 2022, Meyer finally notified its current and former employees of the Data Breach ("Breach Notice")— nearly four months after the Data Breach and three months after Conti's publication of the data.[8]

26. Despite "investigating" the Data Breach for several months, Meyer's Breach Notice revealed little about the breach and obfuscated its nature. Indeed, the Breach Notice misinforms employees that Meyer has "no evidence that [their] specific information was actually accessed or impacted." That statement is untrue as Meyer had reason to know the Conti cybercriminals had, in fact, stolen employee PII as evidenced by Conti's publication of some of the data on the internet.

27. Meyer's Breach Notice assures employees that "The security of [its] employees' information is a top priority," telling them that Meyer has "taken steps to further enhance [its] security controls, and continue[s] to investigate and evaluate [the Data Breach] to prevent a similar occurrence in the future"—steps that should have taken place *before* the Data Breach.

28. Meyer's Breach Notice informs Data Breach victims they can sign up for 24 months of free credit monitoring, which does not adequately address the lifelong harm that the Data Breach poses to its victims.

29. Meyer's Breach Notice does not explain how the hack happened, why it took so long for Meyer to discover it, that cybercriminals have posted employee PII online, what exactly cybercriminals stole, and why it took Meyer nearly 4 months to disclose the breach in a bare-bones

---

[6] *Id.*

[7] *See* https://www.techradar.com/news/meyer-hit-by-ransomware-attack-thousands-of-employees-affected (last visited Mar. 23, 2022).

[8] A true and accurate copy of the Breach Notice is attached as **Exhibit A.**

notice.

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

c. Plaintiff's Experience

31. Plaintiff Brasch is a former Meyer employee, having worked as a biologist in the company's Hestan Smart Cooking division from March 2018 until April 2019.

32. As a condition of Meyer's employment, Meyer required Plaintiff Brasch to provide her PII.

33. Plaintiff Brasch provided her PII to Meyer and trusted that the company would use reasonable measures to protect it according to Meyer's internal policies, as well as state and federal law.

34. Plaintiff Brasch called 888-292-0076—the toll-free phone number listed on Meyer's data breach notice—and Meyer confirmed that her information was part of the breach.

35. In late 2021, an unknown third-party attempted to create a Sprint wireless account in Plaintiff Brasch's name. Given the close proximity between the data breach and this attempted identity theft, it is reasonable to infer that Plaintiff Brasch's PII has already been accessed by criminals as a result of the data breach.

36. Plaintiff Brasch has and will spend considerable time and effort monitoring her accounts to protect herself from identity theft. Plaintiff fears for her personal financial security and uncertainty over what PII was exposed in the Data Breach. Plaintiff 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.

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

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

38. As a result of Meyer'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.

39. 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.

40. The value of Plaintiff 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.

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

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

43. Cybercriminals 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.

44. The development of "Fullz" packages means that stolen PII from the Data Breach can easily be used to link and identify it to Plaintiff 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 cybercriminals 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 and other members of the proposed Class's stolen PII is being misused, and that such misuse is fairly traceable to the Data Breach.

45. 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.

46. Defendant's failure to properly notify Plaintiff and members of the proposed Class of the Data Breach exacerbated Plaintiff and members of the proposed Class's injury 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.

CLASS ACTION ALLEGATIONS

47. Under Cal. Code Civ. P. § 382, Plaintiff sues on behalf of herself and the proposed Class ("Class"), defined as follows:

> All individuals residing in the State of California whose PII was

compromised in the Data Breach disclosed by Meyer in February 2022.

Excluded from the Class are 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.

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

49. *Ascertainability*. Meyer has identified, or is able to identify, all individuals affected by the data breach. These records will identify the Class Members.

50. *Numerosity*. The class includes at least 2,747 class members, so individual joinder would be impracticable.

51. *Well-Defined Community of Interest.* The class constitutes a well-defined community of interest, as demonstrated by the predominance of common issues, the typicality of Plaintiffs' claims to those of the class, the adequacy of Plaintiffs and their counsel as class representatives, and the superiority of representative litigation to individual joinder.

a. **Commonality and Predominance.** This case presents questions of law and fact common to all class members, and those common questions predominate over individualized issues. These common questions include:

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

ii. 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;

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

iv. Whether Defendant breached contractual promises to safeguard Plaintiff and the Class's PII;

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

vi. Whether Defendant's Breach Notice was reasonable;

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

viii. What the proper damages measure is; and

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

b. **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.

c. **Adequacy**. Plaintiff will fairly and adequately protect the proposed Class's interests. Her interests do not conflict with Class members' interests and she 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.

d. **Superiority.** 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 individuals are insufficient to make individual lawsuits economically feasible.

COUNT I

Negligence

(On Behalf of Plaintiff and the Class)

52. Plaintiff realleges all previous paragraphs as if fully set forth below.

53. Plaintiff and members of the Class entrusted their PII to Defendant. Defendant owed to Plaintiff and other members of the Class a duty to exercise reasonable care in handling and using the PII in its care and custody, including by implementing industry-standard security procedures sufficient to reasonably protect the information from the Data Breach, theft, and unauthorized use that came to pass, and to promptly detect attempts at unauthorized access.

54. Defendant owed a duty of care to Plaintiff and members of the Class because it was foreseeable that Defendant's failure to adequately safeguard their PII in accordance with state-of-the-art industry standards concerning data security would result in the compromise of that PII—just like the Data Breach that ultimately came to pass. Defendant acted with wanton and reckless

disregard for the security and confidentiality of Plaintiff's and members of the Class's PII by disclosing and providing access to this information to third parties and by failing to properly supervise both the way the PII was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

55. Defendant owed to Plaintiff and members of the Class a duty to notify them within a reasonable timeframe of any breach to the security of their PII. Defendant also owed a duty to timely and accurately disclose to Plaintiff and members of the Class the scope, nature, and occurrence of the Data Breach. This duty is required and necessary for Plaintiff and members of the Class to take appropriate measures to protect their PII, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

56. Defendant owed these duties to Plaintiff and members of the Class because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security protocols. Defendant actively sought and obtained Plaintiff's and members of the Class's personal information and PII.

57. The risk that unauthorized persons would attempt to gain access to the PII and misuse it was foreseeable. Given that Defendant holds vast amounts of PII, it was inevitable that unauthorized individuals would attempt to access Defendant's databases containing the PII—whether by malware or otherwise.

58. PII is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the PII of Plaintiff and members of the Class and the importance of exercising reasonable care in handling it.

59. Defendant breached its duties by failing to exercise reasonable care in supervising its agents, contractors, vendors, and suppliers, and in handling and securing the personal information and PII of Plaintiff and members of the Class which actually and proximately caused the Data Breach and Plaintiff's and members of the Class's injury.

60. Defendant further breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiff and members of the Class, which actually and proximately caused and

exacerbated the harm from the Data Breach and Plaintiff's and members of the Class's injuries-in-fact.

61. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiff and members of the Class have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

62. Defendant's breach of its common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiff and members of the Class actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their PII by criminals, improper disclosure of their PII, lost benefit of their bargain, lost value of their PII, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendant's negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

COUNT II

Negligence Per Se

(On Behalf of Plaintiff and the Class)

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

64. 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.

65. 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 customers or, in this case, employees' 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 members of the Class's sensitive PII.

66. Defendant violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect its employees' 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 its employees in the event of a breach, which ultimately came to pass.

67. 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 members of the Class.

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

69. 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 and members of the Class's PII.

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

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

72. The injury and harm suffered by Plaintiff and members of the Class were the reasonably foreseeable result of Defendant's breach of its 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.

73. Had Plaintiff and members of the Class known that Defendant would not adequately protect their PII, Plaintiff and members of the Class would not have entrusted Defendant with their PII.

74. As a direct and proximate result of Defendant's negligence per se, Plaintiff and members of 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 their PII; unreimbursed losses relating to fraudulent charges; losses relating to

exceeding credit and debit card limits and balances; 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 an Implied Contract

(On Behalf of Plaintiff and the Class)

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

76. Defendant offered to employ Plaintiff and members of the Class in exchange for their PII.

77. In turn, and through internal policies, Defendant agreed it would not disclose the PII it collects to unauthorized persons. Defendant also promised to safeguard employee PII.

78. Plaintiff and the members of the Class accepted Defendant's offer by providing PII to Defendant in exchange for employment with Defendant.

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

80. Plaintiff and the members of the Class would not have entrusted their PII to Defendant in the absence of such agreement with Defendant.

81. Defendant materially breached the contract(s) it had entered with Plaintiff and members of the Class by failing to safeguard such information and failing to notify them promptly of the intrusion into its computer systems that compromised such information. Defendant further breached the implied contracts with Plaintiff and members of the Class by:

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

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

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

82. The damages sustained by Plaintiff and members of the Class as described above were the direct and proximate result of Defendant's material breaches of its agreement(s).

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

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

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

86. Defendant failed to advise Plaintiff and members of the Class of the Data Breach promptly and sufficiently.

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

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

COUNT IV

Unjust Enrichment

(On Behalf of Plaintiff and the Class)

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

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

91. Plaintiff and members of the Class conferred a benefit upon Defendant in the form of services through employment. Defendant also benefited from the receipt of Plaintiff's and members of the Class's PII, as this was used to facilitate their employment.

92. Defendant appreciated or had knowledge of the benefits conferred upon itself by Plaintiff and members of the Class.

93. Under principals of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiff and the proposed Class's services and their PII because Defendant failed to adequately protect their PII. Plaintiff and the proposed Class would not have provided their PII or worked for Defendant at the payrates they did had they known Defendant would not adequately protect their PII.

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

COUNT V

Violation of California's Consumer Records Act

Cal. Civ. Code § 1798.80, *et seq.*

(On behalf of Plaintiff and the Class)

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

96. Under California law, any "person or business that conducts business in California, and that owns or licenses computerized data that includes personal information" must "disclose any breach of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person." (Cal. Civ. Code § 1798.82.) The disclosure must "be made in the most expedient time possible and without unreasonable delay" (*Id.*), but "immediately following discovery [of the breach], if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person." (Cal. Civ. Code § 1798.82, subdiv. b.)

97. The Data Breach constitutes a "breach of the security system" of Defendant.

98. An unauthorized person acquired the personal, unencrypted information of Plaintiff and the Class.

99. Defendant knew that an unauthorized person had acquired the personal, unencrypted

information of Plaintiff and the Class, but waited approximately three months to notify them. Three months is an unreasonable delay under the circumstances.

100. Defendant's unreasonable delay prevented Plaintiff and the Class from taking appropriate measures from protecting themselves against harm.

101. Because Plaintiff and the Class were unable to protect themselves, they suffered incrementally increased damages that they would not have suffered with timelier notice.

102. Plaintiff and the Class are entitled to equitable relief and damages in an amount to be determined at trial.

COUNT VI

Violation of California's Unfair Competition Law

Cal. Bus. Code § 17200, *et seq.*

(On behalf of Plaintiff and the Class)

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

104. Defendant engaged in unlawful and unfair business practices in violation of Cal. Bus. & Prof. Code § 17200, *et seq*. which prohibits unlawful, unfair, or fraudulent business acts or practices ("UCL").

105. Defendant's conduct is unlawful because it violates the California Consumer Privacy Act of 2018, Civ. Code § 1798.100, *et seq*. (the "CCPA"), and other state data security laws.

106. Defendant stored the PII of Plaintiff and the Class in its computer systems and knew or should have known it did not employ reasonable, industry standard, and appropriate security measures that complied with applicable regulations and that would have kept Plaintiff's and the Class's PII secure so as to prevent the loss or misuse of that PII.

107. Defendant failed to disclose to Plaintiff and the Class that their PII was not secure. However, Plaintiff and the Class were entitled to assume, and did assume, that Defendant had secured their PII. At no time were Plaintiff and the Class on notice that their PII was not secure, which Defendant had a duty to disclose.

108. Defendant also violated California Civil Code § 1798.150 by failing to implement and maintain reasonable security procedures and practices, resulting in an unauthorized access and exfiltration, theft, or disclosure of Plaintiff's and the Class's nonencrypted and nonredacted PII.

109. Had Defendant complied with these requirements, Plaintiff and the Class would not have suffered the damages related to the data breach.

110. Defendant's conduct was unlawful, in that it violated the CCPA.

111. Defendant's conduct was also unfair, in that it violated a clear legislative policy in favor of protecting consumers from data breaches.

112. Defendant's conduct is an unfair business practice under the UCL because it was immoral, unethical, oppressive, and unscrupulous and caused substantial harm. This conduct includes employing unreasonable and inadequate data security despite its business model of actively collecting PII.

113. Defendant also engaged in unfair business practices under the "tethering test." Its actions and omissions, as described above, violated fundamental public policies expressed by the California Legislature. *See, e.g.*, Cal. Civ. Code § 1798.1 ("The Legislature declares that . . . all individuals have a right of privacy in information pertaining to them . . . The increasing use of computers . . . has greatly magnified the potential risk to individual privacy that can occur from the maintenance of personal information."); Cal. Civ. Code § 1798.81.5(a) ("It is the intent of the Legislature to ensure that personal information about California residents is protected."); Cal. Bus. & Prof. Code § 22578 ("It is the intent of the Legislature that this chapter [including the Online Privacy Protection Act] is a matter of statewide concern."). Defendant's acts and omissions thus amount to a violation of the law.

114. Instead, Defendant made the PII of Plaintiff and the Class accessible to scammers, identity thieves, and other malicious actors, subjecting Plaintiff and the Class to an impending risk of identity theft. Additionally, Defendant's conduct was unfair under the UCL because it violated the policies underlying the laws set out in the prior paragraph.

115. As a result of those unlawful and unfair business practices, Plaintiff and the Class suffered an injury-in-fact and have lost money or property.

116. The injuries to Plaintiff and the Class greatly outweigh any alleged countervailing benefit to consumers or competition under all of the circumstances.

117. There were reasonably available alternatives to further Defendant's legitimate business interests, other than the misconduct alleged in this complaint.

118. Therefore, Plaintiff and the Class are entitled to equitable relief, including restitution of all monies paid to or received by Defendant; disgorgement of all profits accruing to Defendant because of its unfair and improper business practices; a permanent injunction enjoining Defendant's unlawful and unfair business activities; and any other equitable relief the Court deems proper.

COUNT VII

Violation of the California Consumer Privacy Act ("CCPA"), Cal. Civ. Code § 1798.150

(On behalf of Plaintiff and the Proposed Class)

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

120. Defendant violated California Civil Code § 1798.150 of the CCPA by failing to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the nonencrypted PII of Plaintiff and the Class. As a direct and proximate result, Plaintiff's, and the Class's nonencrypted and nonredacted PII was subject to unauthorized access and exfiltration, theft, or disclosure.

121. Defendant is a business organized for the profit and financial benefit of its owners according to California Civil Code § 1798.140, that collects the personal information of its employees and whose annual gross revenues exceed the threshold established by California Civil Code § 1798.140(d).

122. Plaintiff and class members seek injunctive or other equitable relief to ensure Defendant hereinafter adequately safeguards PII by implementing reasonable security procedures and practices. Such relief is particularly important because Defendant continues to hold PII, including Plaintiff's and Class members' PII. Plaintiff and Class members have an interest in ensuring that their PII is reasonably protected, and Defendant has demonstrated a pattern of failing to adequately safeguard this information.

123. Pursuant to California Civil Code § 1798.150(b), Plaintiff will send by certified mail a CCPA notice letter to Defendant's registered service agents, identifying the specific provisions of the CCPA that Defendant has violated and continues to violate. If Defendant cannot cure within 30 days of when the letter is delivered—and a cure is not possible under these facts and circumstances—then Plaintiff intends to promptly amend this Complaint to seek statutory damages as permitted by the CCPA.

124. As described herein, an actual controversy has arisen and now exists as to whether Defendant implemented and maintained reasonable security procedures and practices appropriate to the nature of the information so as to protect the personal information under the CCPA.

125. A judicial determination of this issue is necessary and appropriate at this time under the circumstances to prevent further data breaches by Defendant.

PRAYER FOR RELIEF

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 their 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: June 16, 2022

Respectfully submitted,

By: *<u>/s/ Michael J. Boyle, Jr.</u>*

MEYER WILSON CO., LPA
Matthew R. Wilson (SBN 290473)
mwilson@meyerwilson.com
Michael J. Boyle, Jr. (SBN 258560)
mboyle@meyerwilson.com
Jared W. Connors (*pro hac vice* to be filed)
jconnors@meyerwilson.com
305 W. Nationwide Blvd
Columbus, OH 43215
Telephone:(614) 224-6000
Facsimile: (614) 224-6066

TURKE & STRAUSS LLP
Raina Borrelli (*pro hac vice* to be filed)
raina@turkestrauss.com
613 Williamson St., #201
Madison, WI 53703
P: (608) 237-1775

MEYER®

Return Mail Processing
PO Box 999
Suwanee, GA 30024

13 1 2546 **********************************SNGLP
SAMPLE A. SAMPLE - L01
APT ABC
123 ANY ST
ANYTOWN, US 12345-6789

February 15, 2022

RE: NOTICE OF DATA BREACH

Dear Sample A. Sample:

We are writing to notify you about a data security incident that may involve information associated with your employee records maintained by Meyer Corporation, U.S. ("Meyer") and to provide you information about steps you can take to help protect your information.

What Happened?

On or around October 25, 2021, Meyer was the victim of a cybersecurity attack by an unauthorized third party that impacted our systems and operations. Upon detecting the attack, Meyer initiated an investigation with the assistance of our cybersecurity experts, including third-party forensic professionals. On or around December 1, 2021, our investigation identified potential unauthorized access to employee information. While we do not currently have evidence that your specific information has been actually accessed or impacted, we want to inform you of this incident so that you may consider taking additional steps to help protect your information.

What Information Was Involved?

The types of personal information that may have been accessed during this incident will depend on the types of information you have provided to your employer, but may include: first and last name; address; date of birth; gender; race/ethnicity; Social Security number; health insurance information; medical condition(s) and diagnoses; random drug screening results; COVID vaccination cards and status; driver's license, passport, or government-issued identification number; Permanent Resident Card and information regarding immigration status; and information regarding your dependents (including Social Security numbers), if applicable that you may have provided to the company in the course of your employment. Again, at this time, we have no evidence that your specific information was actually accessed or impacted.

What We Are Doing

The security of our employees' information is a top priority, and we are committed to the protection of your information. To help you further protect your information, we are providing you free identity protection services for 2 years, as detailed below. In addition, if you submitted dependent information to

your employer, we are also offering identity protection services for your dependent(s). We have also taken steps to further enhance our security controls, and we continue to investigate and evaluate this matter to prevent a similar occurrence in the future.

What You Can Do

We recommend that you enroll in the identity protection services we are offering to you and your dependents, at no charge. To help protect your identity, we are offering a complimentary 24-month membership of Experian's® IdentityWorks℠. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by**: **April 30, 2022** (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: **www.experianidworks.com/credit**
- Provide your **activation code**: **HFX8G39K2**

If you have a minor dependent, to help protect your minor's identity, we are offering a complimentary 24-month membership of Experian's® IdentityWorks℠. To activate this membership and start monitoring your minor's personal information, please follow the steps below:

- Ensure that you **enroll by**: **April 30, 2022** (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: **www.experianidworks.com/minorplus**
- Provide your **activation code**: **MBL8K25K6**
- Provide your minor's information when prompted

If you have questions about the product, need assistance with identity restoration for you or your minor, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at **(888) 292-0076** by **April 30, 2022**. Be prepared to provide engagement number **B023622** (**B023623** for minors) as proof of eligibility for the identity restoration services by Experian. Additional information regarding Experian IdentityWorks is enclosed.

Other Important Information

There are additional actions you can consider taking to protect your information. We have provided resources where you can obtain additional information about identity theft and ways to protect yourself in the enclosed attachment.

For More Information

We encourage you to take advantage of the identity protection services we are offering to you and your dependents at no charge. Should you have questions or concerns regarding this matter and/or the protections available to you, please call (888) 292-0076 toll-free Monday through Friday from 8 am – 10 pm Central, or Saturday and Sunday from 10 am – 7 pm Central (excluding major U.S. holidays).

Sincerely,

Chris Banning

Chris Banning
Managing Director

ADDITIONAL DETAILS REGARDING THE 24-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP

A credit card is not required for enrollment in Experian IdentityWorks.

You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup**: See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring**: Actively monitors Experian file for indicators of fraud.
- **Identity Restoration**: Identity Restoration agents are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™**: You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to $1 Million Identity Theft Insurance****: Provides coverage for certain costs and unauthorized electronic fund transfers.

You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks for your minor:

- **Social Security Number Trace**: Monitoring to determine whether enrolled minors in your household have an Experian credit report. Alerts of all names, aliases and addresses that become associated with your minor's Social Security Number (SSN) on the Experian credit report.
- **Internet Surveillance**: Technology searches the web, chat rooms & bulletin boards 24/7 to identify trading or selling of your personal information on the Dark Web.
- **Identity Restoration**: Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™**: Receive the same high-level of Identity Restoration support even after the Experian IdentityWorks membership has expired.
- **Up to $1 Million Identity Theft Insurance****: Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your or your minor's information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at (888) 292-0076. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to you for 24 months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

** Offline members will be eligible to call for additional reports quarterly after enrolling.*

*** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.*

ADDITIONAL RESOURCES

The following provides additional information and actions you can consider taking to help protect your information. You may also contact the U.S. Federal Trade Commission ("FTC"), the credit reporting agencies, or your state's regulatory authority to obtain additional information about avoiding identity theft, including information about fraud alerts and security freezes, as further detailed below. Contact Information for the Federal Trade Commission and credit reporting agencies is set forth below:

Federal Trade Commission		
Federal Trade Commission Consumer Response Center 600 Pennsylvania Avenue, NW Washington, DC 20580 1-877-IDTHEFT (438-4338) www.ftc.gov/idtheft		
Credit Reporting Agencies		
Equifax P.O. Box 740241 Atlanta, GA 30374 1-800-525-6285 www.equifax.com	**Experian** P.O. Box 4500 Allen, TX 75013 1-888-397-3742 www.experian.com	**TransUnion** P.O. Box 2000 Chester, PA 19016 1-800-680-7289 www.transunion.com

Order Your Free Annual Credit Report. You can order your free annual credit report online at www.annualcreditreport.com, by phone (toll free) at 877-322-8228, or by mail by submitting a completed Annual Credit Report Request Form to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You can download a copy of the request form on the FTC website: www.ftc.gov. You can also visit the Consumer Financial Protection Bureau's website for more information on how you can obtain your credit report for free: www.consumerfinance.gov. Once you receive your credit reports, review them carefully for any discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting agency.

Review Your Accounts and Report Unauthorized Activity. We recommend you remain vigilant with respect to reviewing your account statements and credit reports, and promptly report any suspicious activity or suspected identity theft to the proper law enforcement authorities, including local law enforcement, your state's attorney general, and/or the FTC. Carefully review your credit reports and bank, credit card, and other account statements. Be proactive and create alerts on credit cards and bank accounts to notify you of activity. If you discover unauthorized or suspicious activity on your credit report or by any other means, file an identity theft report with your local police and contact a credit reporting company. You may also consider filing or obtaining a police report.

We recommend that you regularly review the explanation of benefits statement that you receive from your insurer. If you see any service that you believe you did not receive, please contact your insurer at the number on the statement. If you do not receive regular explanation of benefits statements, contact your provider and request them to send such statements following the provision of services in your name or number.

You may want to order copies of your credit reports and check for any medical bills that you do not recognize. If you find anything suspicious, call the credit reporting agency at the phone number on the report. Keep a copy of this notice for your records in case of future problems with your medical records. You may also want to request a copy of your medical records from your provider, to serve as a baseline. If you are a California resident, we suggest that you visit the web site of the California Office of Privacy Protection at www.privacy.ca.gov to find more information about your medical privacy.

Consider Placing a Fraud Alert on Your Credit File. To protect yourself from potential identity theft, you may consider placing a fraud alert on your credit file. A fraud alert is intended to make it more difficult for someone to open a new credit account in your name. A fraud alert indicates to an entity requesting your credit file that you suspect you are a victim of fraud. When you or someone else attempts to open a credit account in your name, increase the credit limit on an existing account, or obtain a new card on an existing account, the alert notifies the entity to take steps to verify your identity. You may contact one of the credit reporting agencies listed above for assistance.

Consider Placing a Security Freeze on Your Credit File. You also may consider implementing a security freeze (also called a "credit freeze"). Placing a freeze on your credit report restricts access to your credit report and will prevent lenders and others from accessing your credit report entirely. This means you (or others) will not be able to open a new credit account while the freeze is in place. You can temporarily lift the credit freeze if you need to apply for new credit. With a security freeze in place, you may be

required to take special steps when you wish to apply for any type of credit. You may contact one of the credit reporting agencies listed above for assistance.

Remain Vigilant and Lookout for Phishing Schemes. We also encourage you to remain vigilant in managing and handling your personal information and be on the lookout for suspicious emails, such as phishing schemes. Phishing schemes are attempts by criminals to steal personal information, including credit card numbers and social security numbers, over email. These attempts are often made by manipulating an email to make it look as if it came from a legitimate source, but which is actually sent by a fraudulent impersonator. Pay particular attention to anyone asking you to click on a link or attachment, especially if the email requests sensitive information, and pay close attention to the email address (e.g., look for misspellings). It is also important that you check the recipient's email address when replying to emails to ensure it is legitimate. Also consider taking steps such as carrying only essential documents with you, being aware of how and with whom you are sharing your personal information, and shredding receipts, statements, and other sensitive information once you no longer need them. In addition, it is a best practice to take steps to protect your online accounts, such as by changing your passwords regularly and not using the same password across multiple accounts.

For Maryland Residents. You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General:

Maryland Office of the Attorney General
Consumer Protection Division
200 St. Paul Place, Baltimore, MD 21202
1-888-743-0023
www.oag.state.md.us

For Massachusetts Residents: You have the right to obtain a police report and to request a security freeze as described above. The credit reporting agencies may require certain personal information (e.g., name, Social Security number, date of birth, address) and valid identification (e.g., government-issued ID and proof of address, paystub or statement) in order to implement your request for a security freeze. There is no fee for requesting, temporarily lifting, or permanently removing a security freeze with any of the consumer reporting agencies.

For North Carolina Residents: You may also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office:

North Carolina Attorney General's Office
Consumer Protection Division
9001 Mail Service Center
Raleigh, NC 27699-9001
1-877-5-NO-SCAM
www.ncdoj.gov

For Rhode Island Residents: You have the right to obtain a police report. You may also obtain information about preventing and avoiding identity theft from the Rhode Island Office of the Attorney General:

Rhode Island Office of the Attorney General
Consumer Protection Unit
150 South Main Street
Providence, RI 02903
1-401-274-4400
riag.ri.gov

HESTAN

Return Mail Processing
PO Box 999
Suwanee, GA 30024

13 1 2535 **********************************SNGLP
SAMPLE A. SAMPLE - L02
APT ABC
123 ANY ST
ANYTOWN, US 12345-6789

February 15, 2022

RE: NOTICE OF DATA BREACH

Dear Sample A. Sample:

We are writing to notify you about a data security incident that may involve information associated with your employee records maintained by Hestan Commercial Corporation ("Hestan Commercial") and to provide you information about steps you can take to help protect your information.

What Happened?

On or around October 25, 2021, Meyer Corporation, U.S. ("Meyer"), Hestan Commercial's parent company, was the victim of a cybersecurity attack by an unauthorized third party that impacted our systems and operations. Upon detecting the attack, Meyer initiated an investigation with the assistance of cybersecurity experts, including third-party forensic professionals. On or around December 1, 2021, the investigation identified potential unauthorized access to employee information. While we do not currently have evidence that your specific information has been actually accessed or impacted, we want to inform you of this incident so that you may consider taking additional steps to help protect your information.

What Information Was Involved?

The types of personal information that may have been accessed during this incident will depend on the types of information you have provided to your employer, but may include: first and last name; address; date of birth; gender; race/ethnicity; Social Security number; health insurance information; medical condition(s) and diagnoses; random drug screening results; COVID vaccination cards and status; driver's license, passport, or government-issued identification number; Permanent Resident Card and information regarding immigration status; and information regarding your dependents (including Social Security numbers), if applicable that you may have provided to the company in the course of your employment. Again, at this time, we have no evidence that your specific information was actually accessed or impacted.

What We Are Doing

The security of our employees' information is a top priority, and we are committed to the protection of your information. To help you further protect your information, we are providing you free identity protection services for 2 years, as detailed below. In addition, if you submitted dependent information to

your employer, we are also offering identity protection services for your dependent(s). We have also taken steps to further enhance our security controls, and we continue to investigate and evaluate this matter to prevent a similar occurrence in the future.

What You Can Do

We recommend that you enroll in the identity protection services we are offering to you and your dependents, at no charge. To help protect your identity, we are offering a complimentary 24-month membership of Experian's® IdentityWorks℠. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by**: **April 30, 2022** (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: **www.experianidworks.com/credit**
- Provide your **activation code**: **HFX8G39K2**

If you have a minor dependent, to help protect your minor's identity, we are offering a complimentary 24-month membership of Experian's IdentityWorks. To activate this membership and start monitoring your minor's personal information, please follow the steps below:

- Ensure that you **enroll by**: **April 30, 2022** (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: **www.experianidworks.com/minorplus**
- Provide your **activation code**: **MBL8K25K6**
- Provide your minor's information when prompted

If you have questions about the product, need assistance with identity restoration for you or your minor, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at **(888) 292-0076** by **April 30, 2022**. Be prepared to provide engagement number **B023622** (**B023623** for minors) as proof of eligibility for the identity restoration services by Experian. Additional information regarding Experian IdentityWorks is enclosed.

Other Important Information

There are additional actions you can consider taking to protect your information. We have provided resources where you can obtain additional information about identity theft and ways to protect yourself in the enclosed attachment.

For More Information

We encourage you to take advantage of the identity protection services we are offering to you and your dependents at no charge. Should you have questions or concerns regarding this matter and/or the protections available to you, please call (888) 292-0076 toll-free Monday through Friday from 8 am – 10 pm Central, or Saturday and Sunday from 10 am – 7 pm Central (excluding major U.S. holidays).

Sincerely,

Eric Deng
President

ADDITIONAL DETAILS REGARDING THE 24-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP

A credit card is not required for enrollment in Experian IdentityWorks.

You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup**: See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring**: Actively monitors Experian file for indicators of fraud.
- **Identity Restoration**: Identity Restoration agents are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™**: You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to $1 Million Identity Theft Insurance****: Provides coverage for certain costs and unauthorized electronic fund transfers.

You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks for your minor:

- **Social Security Number Trace**: Monitoring to determine whether enrolled minors in your household have an Experian credit report. Alerts of all names, aliases and addresses that become associated with your minor's Social Security Number (SSN) on the Experian credit report.
- **Internet Surveillance**: Technology searches the web, chat rooms & bulletin boards 24/7 to identify trading or selling of your personal information on the Dark Web.
- **Identity Restoration**: Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™**: Receive the same high-level of Identity Restoration support even after the Experian IdentityWorks membership has expired.
- **Up to $1 Million Identity Theft Insurance****: Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your or your minor's information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at (888) 292-0076. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to you for 24 months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

** Offline members will be eligible to call for additional reports quarterly after enrolling.*

*** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.*

ADDITIONAL RESOURCES

The following provides additional information and actions you can consider taking to help protect your information. You may also contact the U.S. Federal Trade Commission ("FTC"), the credit reporting agencies, or your state's regulatory authority to obtain additional information about avoiding identity theft, including information about fraud alerts and security freezes, as further detailed below. Contact Information for the Federal Trade Commission and credit reporting agencies is set forth below:

Federal Trade Commission		
Federal Trade Commission Consumer Response Center 600 Pennsylvania Avenue, NW Washington, DC 20580 1-877-IDTHEFT (438-4338) www.ftc.gov/idtheft		
Credit Reporting Agencies		
Equifax P.O. Box 740241 Atlanta, GA 30374 1-800-525-6285 www.equifax.com	**Experian** P.O. Box 4500 Allen, TX 75013 1-888-397-3742 www.experian.com	**TransUnion** P.O. Box 2000 Chester, PA 19016 1-800-680-7289 www.transunion.com

Order Your Free Annual Credit Report. You can order your free annual credit report online at www.annualcreditreport.com, by phone (toll free) at 877-322-8228, or by mail by submitting a completed Annual Credit Report Request Form to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You can download a copy of the request form on the FTC website: www.ftc.gov. You can also visit the Consumer Financial Protection Bureau's website for more information on how you can obtain your credit report for free: www.consumerfinance.gov. Once you receive your credit reports, review them carefully for any discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting agency.

Review Your Accounts and Report Unauthorized Activity. We recommend you remain vigilant with respect to reviewing your account statements and credit reports, and promptly report any suspicious activity or suspected identity theft to the proper law enforcement authorities, including local law enforcement, your state's attorney general, and/or the FTC. Carefully review your credit reports and bank, credit card, and other account statements. Be proactive and create alerts on credit cards and bank accounts to notify you of activity. If you discover unauthorized or suspicious activity on your credit report or by any other means, file an identity theft report with your local police and contact a credit reporting company. You may also consider filing or obtaining a police report.

We recommend that you regularly review the explanation of benefits statement that you receive from your insurer. If you see any service that you believe you did not receive, please contact your insurer at the number on the statement. If you do not receive regular explanation of benefits statements, contact your provider and request them to send such statements following the provision of services in your name or number.

You may want to order copies of your credit reports and check for any medical bills that you do not recognize. If you find anything suspicious, call the credit reporting agency at the phone number on the report. Keep a copy of this notice for your records in case of future problems with your medical records. You may also want to request a copy of your medical records from your provider, to serve as a baseline. If you are a California resident, we suggest that you visit the web site of the California Office of Privacy Protection at www.privacy.ca.gov to find more information about your medical privacy.

Consider Placing a Fraud Alert on Your Credit File. To protect yourself from potential identity theft, you may consider placing a fraud alert on your credit file. A fraud alert is intended to make it more difficult for someone to open a new credit account in your name. A fraud alert indicates to an entity requesting your credit file that you suspect you are a victim of fraud. When you or someone else attempts to open a credit account in your name, increase the credit limit on an existing account, or obtain a new card on an existing account, the alert notifies the entity to take steps to verify your identity. You may contact one of the credit reporting agencies listed above for assistance.

Consider Placing a Security Freeze on Your Credit File. You also may consider implementing a security freeze (also called a "credit freeze"). Placing a freeze on your credit report restricts access to your credit report and will prevent lenders and others from accessing your credit report entirely. This means you (or others) will not be able to open a new credit account while the freeze is in place. You can temporarily lift the credit freeze if you need to apply for new credit. With a security freeze in place, you may be

required to take special steps when you wish to apply for any type of credit. You may contact one of the credit reporting agencies listed above for assistance.

Remain Vigilant and Lookout for Phishing Schemes. We also encourage you to remain vigilant in managing and handling your personal information and be on the lookout for suspicious emails, such as phishing schemes. Phishing schemes are attempts by criminals to steal personal information, including credit card numbers and social security numbers, over email. These attempts are often made by manipulating an email to make it look as if it came from a legitimate source, but which is actually sent by a fraudulent impersonator. Pay particular attention to anyone asking you to click on a link or attachment, especially if the email requests sensitive information, and pay close attention to the email address (e.g., look for misspellings). It is also important that you check the recipient's email address when replying to emails to ensure it is legitimate. Also consider taking steps such as carrying only essential documents with you, being aware of how and with whom you are sharing your personal information, and shredding receipts, statements, and other sensitive information once you no longer need them. In addition, it is a best practice to take steps to protect your online accounts, such as by changing your passwords regularly and not using the same password across multiple accounts.

For Maryland Residents. You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General:

Maryland Office of the Attorney General
Consumer Protection Division
200 St. Paul Place, Baltimore, MD 21202
1-888-743-0023
www.oag.state.md.us

For Massachusetts Residents: You have the right to obtain a police report and to request a security freeze as described above. The credit reporting agencies may require certain personal information (e.g., name, Social Security number, date of birth, address) and valid identification (e.g., government-issued ID and proof of address, paystub or statement) in order to implement your request for a security freeze. There is no fee for requesting, temporarily lifting, or permanently removing a security freeze with any of the consumer reporting agencies.

For North Carolina Residents: You may also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office:

North Carolina Attorney General's Office
Consumer Protection Division
9001 Mail Service Center
Raleigh, NC 27699-9001
1-877-5-NO-SCAM
www.ncdoj.gov

For Rhode Island Residents: You have the right to obtain a police report. You may also obtain information about preventing and avoiding identity theft from the Rhode Island Office of the Attorney General:

Rhode Island Office of the Attorney General
Consumer Protection Unit
150 South Main Street
Providence, RI 02903
1-401-274-4400
riag.ri.gov

HESTAN CUE™
SMART COOKING SYSTEM

Return Mail Processing
PO Box 999
Suwanee, GA 30024

13 1 2547 **********************************SNGLP
SAMPLE A. SAMPLE - L05
APT ABC
123 ANY ST
ANYTOWN, US 12345-6789

February 15, 2022

RE: NOTICE OF DATA BREACH

Dear Sample A. Sample:

We are writing to notify you about a data security incident that may involve information associated with your employee records maintained by Hestan Smart Cooking Inc. ("Hestan Smart Cooking") and to provide you information about steps you can take to help protect your information.

<u>What Happened?</u>

On or around October 25, 2021, Meyer Corporation, U.S. ("Meyer"), Hestan Smart Cooking's parent company, was the victim of a cybersecurity attack by an unauthorized third party that impacted our systems and operations. Upon detecting the attack, Meyer initiated an investigation with the assistance of cybersecurity experts, including third-party forensic professionals. On or around December 1, 2021, the investigation identified potential unauthorized access to employee information. While we do not currently have evidence that your specific information has been actually accessed or impacted, we want to inform you of this incident so that you may consider taking additional steps to help protect your information.

<u>What Information Was Involved?</u>

The types of personal information that may have been accessed during this incident will depend on the types of information you have provided to your employer, but may include: first and last name; address; date of birth; gender; race/ethnicity; Social Security number; health insurance information; medical condition(s) and diagnoses; random drug screening results; COVID vaccination cards and status; driver's license, passport, or government-issued identification number; Permanent Resident Card and information regarding immigration status; and information regarding your dependents (including Social Security numbers), if applicable that you may have provided to the company in the course of your employment. Again, at this time, we have no evidence that your specific information was actually accessed or impacted.

<u>What We Are Doing</u>

The security of our employees' information is a top priority, and we are committed to the protection of your information. To help you further protect your information, we are providing you free identity protection services for 2 years, as detailed below. In addition, if you submitted dependent information to

your employer, we are also offering identity protection services for your dependent(s). We have also taken steps to further enhance our security controls, and we continue to investigate and evaluate this matter to prevent a similar occurrence in the future.

What You Can Do

We recommend that you enroll in the identity protection services we are offering to you and your dependents, at no charge. To help protect your identity, we are offering a complimentary 24-month membership of Experian's® IdentityWorks℠. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by**: **April 30, 2022** (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: **www.experianidworks.com/credit**
- Provide your **activation code**: **HFX8G39K2**

If you have a minor dependent, to help protect your minor's identity, we are offering a complimentary 24-month membership of Experian's IdentityWorks. To activate this membership and start monitoring your minor's personal information, please follow the steps below:

- Ensure that you **enroll by**: **April 30, 2022** (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: **www.experianidworks.com/minorplus**
- Provide your **activation code**: **MBL8K25K6**
- Provide your minor's information when prompted

If you have questions about the product, need assistance with identity restoration for you or your minor, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at **(888) 292-0076** by **April 30, 2022**. Be prepared to provide engagement number **B023622** (**B023623** for minors) as proof of eligibility for the identity restoration services by Experian. Additional information regarding Experian IdentityWorks is enclosed.

Other Important Information

There are additional actions you can consider taking to protect your information. We have provided resources where you can obtain additional information about identity theft and ways to protect yourself in the enclosed attachment.

For More Information

We encourage you to take advantage of the identity protection services we are offering to you and your dependents at no charge. Should you have questions or concerns regarding this matter and/or the protections available to you, please call (888) 292-0076 toll-free Monday through Friday from 8 am – 10 pm Central, or Saturday and Sunday from 10 am – 7 pm Central (excluding major U.S. holidays).

Sincerely,

Scott Kim
Managing Director

ADDITIONAL DETAILS REGARDING THE 24-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP

A credit card is not required for enrollment in Experian IdentityWorks.

You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup**: See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring**: Actively monitors Experian file for indicators of fraud.
- **Identity Restoration**: Identity Restoration agents are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™**: You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to $1 Million Identity Theft Insurance****: Provides coverage for certain costs and unauthorized electronic fund transfers.

You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks for your minor:

- **Social Security Number Trace**: Monitoring to determine whether enrolled minors in your household have an Experian credit report. Alerts of all names, aliases and addresses that become associated with your minor's Social Security Number (SSN) on the Experian credit report.
- **Internet Surveillance**: Technology searches the web, chat rooms & bulletin boards 24/7 to identify trading or selling of your personal information on the Dark Web.
- **Identity Restoration**: Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™**: Receive the same high-level of Identity Restoration support even after the Experian IdentityWorks membership has expired.
- **Up to $1 Million Identity Theft Insurance****: Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your or your minor's information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at (888) 292-0076. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to you for 24 months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

** Offline members will be eligible to call for additional reports quarterly after enrolling.*

*** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.*

ADDITIONAL RESOURCES

The following provides additional information and actions you can consider taking to help protect your information. You may also contact the U.S. Federal Trade Commission ("FTC"), the credit reporting agencies, or your state's regulatory authority to obtain additional information about avoiding identity theft, including information about fraud alerts and security freezes, as further detailed below. Contact Information for the Federal Trade Commission and credit reporting agencies is set forth below:

Federal Trade Commission		
Federal Trade Commission Consumer Response Center 600 Pennsylvania Avenue, NW Washington, DC 20580 1-877-IDTHEFT (438-4338) www.ftc.gov/idtheft		
Credit Reporting Agencies		
Equifax P.O. Box 740241 Atlanta, GA 30374 1-800-525-6285 www.equifax.com	**Experian** P.O. Box 4500 Allen, TX 75013 1-888-397-3742 www.experian.com	**TransUnion** P.O. Box 2000 Chester, PA 19016 1-800-680-7289 www.transunion.com

Order Your Free Annual Credit Report. You can order your free annual credit report online at www.annualcreditreport.com, by phone (toll free) at 877-322-8228, or by mail by submitting a completed Annual Credit Report Request Form to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You can download a copy of the request form on the FTC website: www.ftc.gov. You can also visit the Consumer Financial Protection Bureau's website for more information on how you can obtain your credit report for free: www.consumerfinance.gov. Once you receive your credit reports, review them carefully for any discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting agency.

Review Your Accounts and Report Unauthorized Activity. We recommend you remain vigilant with respect to reviewing your account statements and credit reports, and promptly report any suspicious activity or suspected identity theft to the proper law enforcement authorities, including local law enforcement, your state's attorney general, and/or the FTC. Carefully review your credit reports and bank, credit card, and other account statements. Be proactive and create alerts on credit cards and bank accounts to notify you of activity. If you discover unauthorized or suspicious activity on your credit report or by any other means, file an identity theft report with your local police and contact a credit reporting company. You may also consider filing or obtaining a police report.

We recommend that you regularly review the explanation of benefits statement that you receive from your insurer. If you see any service that you believe you did not receive, please contact your insurer at the number on the statement. If you do not receive regular explanation of benefits statements, contact your provider and request them to send such statements following the provision of services in your name or number.

You may want to order copies of your credit reports and check for any medical bills that you do not recognize. If you find anything suspicious, call the credit reporting agency at the phone number on the report. Keep a copy of this notice for your records in case of future problems with your medical records. You may also want to request a copy of your medical records from your provider, to serve as a baseline. If you are a California resident, we suggest that you visit the web site of the California Office of Privacy Protection at www.privacy.ca.gov to find more information about your medical privacy.

Consider Placing a Fraud Alert on Your Credit File. To protect yourself from potential identity theft, you may consider placing a fraud alert on your credit file. A fraud alert is intended to make it more difficult for someone to open a new credit account in your name. A fraud alert indicates to an entity requesting your credit file that you suspect you are a victim of fraud. When you or someone else attempts to open a credit account in your name, increase the credit limit on an existing account, or obtain a new card on an existing account, the alert notifies the entity to take steps to verify your identity. You may contact one of the credit reporting agencies listed above for assistance.

Consider Placing a Security Freeze on Your Credit File. You also may consider implementing a security freeze (also called a "credit freeze"). Placing a freeze on your credit report restricts access to your credit report and will prevent lenders and others from accessing your credit report entirely. This means you (or others) will not be able to open a new credit account while the freeze is in place. You can temporarily lift the credit freeze if you need to apply for new credit. With a security freeze in place, you may be required to take special steps when you wish to apply for any type of credit. You may contact one of the credit reporting agencies listed above for assistance.

Remain Vigilant and Lookout for Phishing Schemes. We also encourage you to remain vigilant in managing and handling your personal information and be on the lookout for suspicious emails, such as phishing schemes. Phishing schemes are attempts by criminals to steal personal information, including credit card numbers and social security numbers, over email. These attempts are often made by manipulating an email to make it look as if it came from a legitimate source, but which is actually sent by a fraudulent impersonator. Pay particular attention to anyone asking you to click on a link or attachment, especially if the email requests sensitive information, and pay close attention to the email address (e.g., look for misspellings). It is also important that you check the recipient's email address when replying to emails to ensure it is legitimate. Also consider taking steps such as carrying only essential documents with you, being aware of how and with whom you are sharing your personal information, and shredding receipts, statements, and other sensitive information once you no longer need them. In addition, it is a best practice to take steps to protect your online accounts, such as by changing your passwords regularly and not using the same password across multiple accounts.

For Maryland Residents. You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General:

Maryland Office of the Attorney General
Consumer Protection Division
200 St. Paul Place, Baltimore, MD 21202
1-888-743-0023
www.oag.state.md.us

For Massachusetts Residents: You have the right to obtain a police report and to request a security freeze as described above. The credit reporting agencies may require certain personal information (e.g., name, Social Security number, date of birth, address) and valid identification (e.g., government-issued ID and proof of address, paystub or statement) in order to implement your request for a security freeze. There is no fee for requesting, temporarily lifting, or permanently removing a security freeze with any of the consumer reporting agencies.

For North Carolina Residents: You may also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office:

North Carolina Attorney General's Office
Consumer Protection Division
9001 Mail Service Center
Raleigh, NC 27699-9001
1-877-5-NO-SCAM
www.ncdoj.gov

For Rhode Island Residents: You have the right to obtain a police report. You may also obtain information about preventing and avoiding identity theft from the Rhode Island Office of the Attorney General:

Rhode Island Office of the Attorney General
Consumer Protection Unit
150 South Main Street
Providence, RI 02903
1-401-274-4400
riag.ri.gov

HESTAN VINEYARDS

Return Mail Processing
PO Box 999
Suwanee, GA 30024

11 1 2334 *****************AUTO**ALL FOR AADC 945
SAMPLE A. SAMPLE - L04
APT ABC
123 ANY ST
ANYTOWN, US 12345-6789

February 15, 2022

RE: NOTICE OF DATA BREACH

Dear Sample A. Sample:

We are writing to notify you about a data security incident that may involve information associated with your employee records maintained by Hestan Vineyards LLC ("Hestan Vineyards") and to provide you information about steps you can take to help protect your information.

What Happened?

On or around October 25, 2021, Meyer Corporation, U.S. ("Meyer"), Hestan Vineyards' parent company, was the victim of a cybersecurity attack by an unauthorized third party that impacted our systems and operations. Upon detecting the attack, Meyer initiated an investigation with the assistance of cybersecurity experts, including third-party forensic professionals. On or around December 1, 2021, the investigation identified potential unauthorized access to employee information. While we do not currently have evidence that your specific information has been actually accessed or impacted, we want to inform you of this incident so that you may consider taking additional steps to help protect your information.

What Information Was Involved?

The types of personal information that may have been accessed during this incident will depend on the types of information you have provided to your employer, but may include: first and last name; address; date of birth; gender; race/ethnicity; Social Security number; health insurance information; medical condition(s) and diagnoses; random drug screening results; COVID vaccination cards and status; driver's license, passport, or government-issued identification number; Permanent Resident Card and information regarding immigration status; and information regarding your dependents (including Social Security numbers), if applicable that you may have provided to the company in the course of your employment. Again, at this time, we have no evidence that your specific information was actually accessed or impacted.

What We Are Doing

The security of our employees' information is a top priority, and we are committed to the protection of your information. To help you further protect your information, we are providing you free identity protection services for 2 years, as detailed below. In addition, if you submitted dependent information to

your employer, we are also offering identity protection services for your dependent(s). We have also taken steps to further enhance our security controls, and we continue to investigate and evaluate this matter to prevent a similar occurrence in the future.

What You Can Do

We recommend that you enroll in the identity protection services we are offering to you and your dependents, at no charge. To help protect your identity, we are offering a complimentary 24-month membership of Experian's® IdentityWorks℠. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by**: **April 30, 2022** (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: **www.experianidworks.com/credit**
- Provide your **activation code**: **HFX8G39K2**

If you have a minor dependent, to help protect your minor's identity, we are offering a complimentary 24-month membership of Experian's IdentityWorks. To activate this membership and start monitoring your minor's personal information, please follow the steps below:

- Ensure that you **enroll by**: **April 30, 2022** (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: **www.experianidworks.com/minorplus**
- Provide your **activation code**: **MBL8K25K6**
- Provide your minor's information when prompted

If you have questions about the product, need assistance with identity restoration for you or your minor, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at **(888) 292-0076** by **April 30, 2022**. Be prepared to provide engagement number **B023622** (**B023623** for minors) as proof of eligibility for the identity restoration services by Experian. Additional information regarding Experian IdentityWorks is enclosed.

Other Important Information

There are additional actions you can consider taking to protect your information. We have provided resources where you can obtain additional information about identity theft and ways to protect yourself in the enclosed attachment.

For More Information

We encourage you to take advantage of the identity protection services we are offering to you and your dependents at no charge. Should you have questions or concerns regarding this matter and/or the protections available to you, please call (888) 292-0076 toll-free Monday through Friday from 8 am – 10 pm Central, or Saturday and Sunday from 10 am – 7 pm Central (excluding major U.S. holidays).

Sincerely,

Ann Hitchcock

Ann Hitchcock
Director of Operations

ADDITIONAL DETAILS REGARDING THE 24-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP

A credit card is not required for enrollment in Experian IdentityWorks.

You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup**: See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring**: Actively monitors Experian file for indicators of fraud.
- **Identity Restoration**: Identity Restoration agents are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™**: You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to $1 Million Identity Theft Insurance****: Provides coverage for certain costs and unauthorized electronic fund transfers.

You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks for your minor:

- **Social Security Number Trace**: Monitoring to determine whether enrolled minors in your household have an Experian credit report. Alerts of all names, aliases and addresses that become associated with your minor's Social Security Number (SSN) on the Experian credit report.
- **Internet Surveillance**: Technology searches the web, chat rooms & bulletin boards 24/7 to identify trading or selling of your personal information on the Dark Web.
- **Identity Restoration**: Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™**: Receive the same high-level of Identity Restoration support even after the Experian IdentityWorks membership has expired.
- **Up to $1 Million Identity Theft Insurance****: Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your or your minor's information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at (888) 292-0076. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to you for 24 months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

** Offline members will be eligible to call for additional reports quarterly after enrolling.*

*** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.*

ADDITIONAL RESOURCES

The following provides additional information and actions you can consider taking to help protect your information. You may also contact the U.S. Federal Trade Commission ("FTC"), the credit reporting agencies, or your state's regulatory authority to obtain additional information about avoiding identity theft, including information about fraud alerts and security freezes, as further detailed below. Contact Information for the Federal Trade Commission and credit reporting agencies is set forth below:

Federal Trade Commission
Federal Trade Commission Consumer Response Center 600 Pennsylvania Avenue, NW Washington, DC 20580 1-877-IDTHEFT (438-4338) www.ftc.gov/idtheft

Credit Reporting Agencies		
Equifax P.O. Box 740241 Atlanta, GA 30374 1-800-525-6285 www.equifax.com	**Experian** P.O. Box 4500 Allen, TX 75013 1-888-397-3742 www.experian.com	**TransUnion** P.O. Box 2000 Chester, PA 19016 1-800-680-7289 www.transunion.com

Order Your Free Annual Credit Report. You can order your free annual credit report online at www.annualcreditreport.com, by phone (toll free) at 877-322-8228, or by mail by submitting a completed Annual Credit Report Request Form to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You can download a copy of the request form on the FTC website: www.ftc.gov. You can also visit the Consumer Financial Protection Bureau's website for more information on how you can obtain your credit report for free: www.consumerfinance.gov. Once you receive your credit reports, review them carefully for any discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting agency.

Review Your Accounts and Report Unauthorized Activity. We recommend you remain vigilant with respect to reviewing your account statements and credit reports, and promptly report any suspicious activity or suspected identity theft to the proper law enforcement authorities, including local law enforcement, your state's attorney general, and/or the FTC. Carefully review your credit reports and bank, credit card, and other account statements. Be proactive and create alerts on credit cards and bank accounts to notify you of activity. If you discover unauthorized or suspicious activity on your credit report or by any other means, file an identity theft report with your local police and contact a credit reporting company. You may also consider filing or obtaining a police report.

We recommend that you regularly review the explanation of benefits statement that you receive from your insurer. If you see any service that you believe you did not receive, please contact your insurer at the number on the statement. If you do not receive regular explanation of benefits statements, contact your provider and request them to send such statements following the provision of services in your name or number.

You may want to order copies of your credit reports and check for any medical bills that you do not recognize. If you find anything suspicious, call the credit reporting agency at the phone number on the report. Keep a copy of this notice for your records in case of future problems with your medical records. You may also want to request a copy of your medical records from your provider, to serve as a baseline. If you are a California resident, we suggest that you visit the web site of the California Office of Privacy Protection at www.privacy.ca.gov to find more information about your medical privacy.

Consider Placing a Fraud Alert on Your Credit File. To protect yourself from potential identity theft, you may consider placing a fraud alert on your credit file. A fraud alert is intended to make it more difficult for someone to open a new credit account in your name. A fraud alert indicates to an entity requesting your credit file that you suspect you are a victim of fraud. When you or someone else attempts to open a credit account in your name, increase the credit limit on an existing account, or obtain a new card on an existing account, the alert notifies the entity to take steps to verify your identity. You may contact one of the credit reporting agencies listed above for assistance.

Consider Placing a Security Freeze on Your Credit File. You also may consider implementing a security freeze (also called a "credit freeze"). Placing a freeze on your credit report restricts access to your credit report and will prevent lenders and others from accessing your credit report entirely. This means you (or others) will not be able to open a new credit account while the freeze is in place. You can temporarily lift the credit freeze if you need to apply for new credit. With a security freeze in place, you may be

required to take special steps when you wish to apply for any type of credit. You may contact one of the credit reporting agencies listed above for assistance.

Remain Vigilant and Lookout for Phishing Schemes. We also encourage you to remain vigilant in managing and handling your personal information and be on the lookout for suspicious emails, such as phishing schemes. Phishing schemes are attempts by criminals to steal personal information, including credit card numbers and social security numbers, over email. These attempts are often made by manipulating an email to make it look as if it came from a legitimate source, but which is actually sent by a fraudulent impersonator. Pay particular attention to anyone asking you to click on a link or attachment, especially if the email requests sensitive information, and pay close attention to the email address (e.g., look for misspellings). It is also important that you check the recipient's email address when replying to emails to ensure it is legitimate. Also consider taking steps such as carrying only essential documents with you, being aware of how and with whom you are sharing your personal information, and shredding receipts, statements, and other sensitive information once you no longer need them. In addition, it is a best practice to take steps to protect your online accounts, such as by changing your passwords regularly and not using the same password across multiple accounts.

For Maryland Residents. You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General:

Maryland Office of the Attorney General
Consumer Protection Division
200 St. Paul Place, Baltimore, MD 21202
1-888-743-0023
www.oag.state.md.us

For Massachusetts Residents: You have the right to obtain a police report and to request a security freeze as described above. The credit reporting agencies may require certain personal information (e.g., name, Social Security number, date of birth, address) and valid identification (e.g., government-issued ID and proof of address, paystub or statement) in order to implement your request for a security freeze. There is no fee for requesting, temporarily lifting, or permanently removing a security freeze with any of the consumer reporting agencies.

For North Carolina Residents: You may also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office:

North Carolina Attorney General's Office
Consumer Protection Division
9001 Mail Service Center
Raleigh, NC 27699-9001
1-877-5-NO-SCAM
www.ncdoj.gov

For Rhode Island Residents: You have the right to obtain a police report. You may also obtain information about preventing and avoiding identity theft from the Rhode Island Office of the Attorney General:

Rhode Island Office of the Attorney General
Consumer Protection Unit
150 South Main Street
Providence, RI 02903
1-401-274-4400
riag.ri.gov

BLUE MOUNTAIN
ENTERPRISES

Return Mail Processing
PO Box 999
Suwanee, GA 30024

13 1 2545 **********************************SNGLP
SAMPLE A. SAMPLE - L03
APT ABC
123 ANY ST
ANYTOWN, US 12345-6789

February 15, 2022

RE: NOTICE OF DATA BREACH

Dear Sample A. Sample:

We are writing to notify you about a data security incident that may involve information associated with your employee records maintained by Blue Mountain Enterprises, LLC ("Blue Mountain") and to provide you information about steps you can take to help protect your information.

<u>What Happened?</u>

On or around October 25, 2021, Meyer Corporation, U.S. ("Meyer"), Blue Mountain's parent company, was the victim of a cybersecurity attack by an unauthorized third party that impacted our systems and operations. Upon detecting the attack, Meyer initiated an investigation with the assistance of cybersecurity experts, including third-party forensic professionals. On or around December 1, 2021, the investigation identified potential unauthorized access to employee information. While we do not currently have evidence that your specific information has been actually accessed or impacted, we want to inform you of this incident so that you may consider taking additional steps to help protect your information.

<u>What Information Was Involved?</u>

The types of personal information that may have been accessed during this incident will depend on the types of information you have provided to your employer, but may include: first and last name; address; date of birth; gender; race/ethnicity; Social Security number; health insurance information; medical condition(s) and diagnoses; random drug screening results; COVID vaccination cards and status; driver's license, passport, or government-issued identification number; Permanent Resident Card and information regarding immigration status; and information regarding your dependents (including Social Security numbers), if applicable that you may have provided to the company in the course of your employment. Again, at this time, we have no evidence that your specific information was actually accessed or impacted.

<u>What We Are Doing</u>

The security of our employees' information is a top priority, and we are committed to the protection of your information. To help you further protect your information, we are providing you free identity protection services for 2 years, as detailed below. In addition, if you submitted dependent information to your employer, we are also offering identity protection services for your dependent(s). We have also taken steps to further enhance our security controls, and we continue to investigate and evaluate this matter to prevent a similar occurrence in the future.

What You Can Do

We recommend that you enroll in the identity protection services we are offering to you and your dependents, at no charge. To help protect your identity, we are offering a complimentary 24-month membership of Experian's® IdentityWorks℠. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by**: **April 30, 2022** (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: **www.experianidworks.com/credit**
- Provide your **activation code**: **HFX8G39K2**

If you have a minor dependent, to help protect your minor's identity, we are offering a complimentary 24-month membership of Experian's IdentityWorks. To activate this membership and start monitoring your minor's personal information, please follow the steps below:

- Ensure that you **enroll by**: **April 30, 2022** (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: **www.experianidworks.com/minorplus**
- Provide your **activation code**: **MBL8K25K6**
- Provide your minor's information when prompted

If you have questions about the product, need assistance with identity restoration for you or your minor, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at **(888) 292-0076** by **April 30, 2022**. Be prepared to provide engagement number **B023622** (**B023623** for minors) as proof of eligibility for the identity restoration services by Experian. Additional information regarding Experian IdentityWorks is enclosed.

Other Important Information

There are additional actions you can consider taking to protect your information. We have provided resources where you can obtain additional information about identity theft and ways to protect yourself in the enclosed attachment.

For More Information

We encourage you to take advantage of the identity protection services we are offering to you and your dependents at no charge. Should you have questions or concerns regarding this matter and/or the protections available to you, please call (888) 292-0076 toll-free Monday through Friday from 8 am – 10 pm Central, or Saturday and Sunday from 10 am – 7 pm Central (excluding major U.S. holidays).

Sincerely,

Stephanie MacLean
Chief Executive Officer

ADDITIONAL DETAILS REGARDING THE 24-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP

A credit card is not required for enrollment in Experian IdentityWorks.

You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup**: See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring**: Actively monitors Experian file for indicators of fraud.
- **Identity Restoration**: Identity Restoration agents are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™**: You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to $1 Million Identity Theft Insurance****: Provides coverage for certain costs and unauthorized electronic fund transfers.

You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks for your minor:

- **Social Security Number Trace**: Monitoring to determine whether enrolled minors in your household have an Experian credit report. Alerts of all names, aliases and addresses that become associated with your minor's Social Security Number (SSN) on the Experian credit report.
- **Internet Surveillance**: Technology searches the web, chat rooms & bulletin boards 24/7 to identify trading or selling of your personal information on the Dark Web.
- **Identity Restoration**: Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™**: Receive the same high-level of Identity Restoration support even after the Experian IdentityWorks membership has expired.
- **Up to $1 Million Identity Theft Insurance****: Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your or your minor's information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at (888) 292-0076. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to you for 24 months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

** Offline members will be eligible to call for additional reports quarterly after enrolling.*

*** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.*

ADDITIONAL RESOURCES

The following provides additional information and actions you can consider taking to help protect your information. You may also contact the U.S. Federal Trade Commission ("FTC"), the credit reporting agencies, or your state's regulatory authority to obtain additional information about avoiding identity theft, including information about fraud alerts and security freezes, as further detailed below. Contact Information for the Federal Trade Commission and credit reporting agencies is set forth below:

Federal Trade Commission		
Federal Trade Commission Consumer Response Center 600 Pennsylvania Avenue, NW Washington, DC 20580 1-877-IDTHEFT (438-4338) www.ftc.gov/idtheft		
Credit Reporting Agencies		
Equifax P.O. Box 740241 Atlanta, GA 30374 1-800-525-6285 www.equifax.com	**Experian** P.O. Box 4500 Allen, TX 75013 1-888-397-3742 www.experian.com	**TransUnion** P.O. Box 2000 Chester, PA 19016 1-800-680-7289 www.transunion.com

Order Your Free Annual Credit Report. You can order your free annual credit report online at www.annualcreditreport.com, by phone (toll free) at 877-322-8228, or by mail by submitting a completed Annual Credit Report Request Form to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You can download a copy of the request form on the FTC website: www.ftc.gov. You can also visit the Consumer Financial Protection Bureau's website for more information on how you can obtain your credit report for free: www.consumerfinance.gov. Once you receive your credit reports, review them carefully for any discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting agency.

Review Your Accounts and Report Unauthorized Activity. We recommend you remain vigilant with respect to reviewing your account statements and credit reports, and promptly report any suspicious activity or suspected identity theft to the proper law enforcement authorities, including local law enforcement, your state's attorney general, and/or the FTC. Carefully review your credit reports and bank, credit card, and other account statements. Be proactive and create alerts on credit cards and bank accounts to notify you of activity. If you discover unauthorized or suspicious activity on your credit report or by any other means, file an identity theft report with your local police and contact a credit reporting company. You may also consider filing or obtaining a police report.

We recommend that you regularly review the explanation of benefits statement that you receive from your insurer. If you see any service that you believe you did not receive, please contact your insurer at the number on the statement. If you do not receive regular explanation of benefits statements, contact your provider and request them to send such statements following the provision of services in your name or number.

You may want to order copies of your credit reports and check for any medical bills that you do not recognize. If you find anything suspicious, call the credit reporting agency at the phone number on the report. Keep a copy of this notice for your records in case of future problems with your medical records. You may also want to request a copy of your medical records from your provider, to serve as a baseline. If you are a California resident, we suggest that you visit the web site of the California Office of Privacy Protection at www.privacy.ca.gov to find more information about your medical privacy.

Consider Placing a Fraud Alert on Your Credit File. To protect yourself from potential identity theft, you may consider placing a fraud alert on your credit file. A fraud alert is intended to make it more difficult for someone to open a new credit account in your name. A fraud alert indicates to an entity requesting your credit file that you suspect you are a victim of fraud. When you or someone else attempts to open a credit account in your name, increase the credit limit on an existing account, or obtain a new card on an existing account, the alert notifies the entity to take steps to verify your identity. You may contact one of the credit reporting agencies listed above for assistance.

Consider Placing a Security Freeze on Your Credit File. You also may consider implementing a security freeze (also called a "credit freeze"). Placing a freeze on your credit report restricts access to your credit report and will prevent lenders and others from accessing your credit report entirely. This means you (or others) will not be able to open a new credit account while the freeze is in place. You can temporarily lift the credit freeze if you need to apply for new credit. With a security freeze in place, you may be required to take special steps when you wish to apply for any type of credit. You may contact one of the credit reporting agencies listed above for assistance.

Remain Vigilant and Lookout for Phishing Schemes. We also encourage you to remain vigilant in managing and handling your personal information and be on the lookout for suspicious emails, such as phishing schemes. Phishing schemes are attempts by criminals to steal personal information, including credit card numbers and social security numbers, over email. These attempts are often made by manipulating an email to make it look as if it came from a legitimate source, but which is actually sent by a fraudulent impersonator. Pay particular attention to anyone asking you to click on a link or attachment, especially if the email requests sensitive information, and pay close attention to the email address (e.g., look for misspellings). It is also important that you check the recipient's email address when replying to emails to ensure it is legitimate. Also consider taking steps such as carrying only essential documents with you, being aware of how and with whom you are sharing your personal information, and shredding receipts, statements, and other sensitive information once you no longer need them. In addition, it is a best practice to take steps to protect your online accounts, such as by changing your passwords regularly and not using the same password across multiple accounts.

For Maryland Residents. You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General:

Maryland Office of the Attorney General
Consumer Protection Division
200 St. Paul Place, Baltimore, MD 21202
1-888-743-0023
www.oag.state.md.us

For Massachusetts Residents: You have the right to obtain a police report and to request a security freeze as described above. The credit reporting agencies may require certain personal information (e.g., name, Social Security number, date of birth, address) and valid identification (e.g., government-issued ID and proof of address, paystub or statement) in order to implement your request for a security freeze. There is no fee for requesting, temporarily lifting, or permanently removing a security freeze with any of the consumer reporting agencies.

For North Carolina Residents: You may also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office:

North Carolina Attorney General's Office
Consumer Protection Division
9001 Mail Service Center
Raleigh, NC 27699-9001
1-877-5-NO-SCAM
www.ncdoj.gov

For Rhode Island Residents: You have the right to obtain a police report. You may also obtain information about preventing and avoiding identity theft from the Rhode Island Office of the Attorney General:

Rhode Island Office of the Attorney General
Consumer Protection Unit
150 South Main Street
Providence, RI 02903
1-401-274-4400
riag.ri.gov

CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. *(SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)*

I. (a) PLAINTIFFS
Madeleine Brasch

DEFENDANTS
Meyer Corporation, U.S.

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

County of Residence of First Listed Defendant: Solano
(IN U.S. PLAINTIFF CASES ONLY)
NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

(c) Attorneys *(Firm Name, Address, and Telephone Number)*
Michael J. Boyle, Jr., Meyer Wilson Co., LPA, 305 W. Nationwide Blvd., Colubmus, OH 43215

Attorneys *(If Known)*

II. BASIS OF JURISDICTION *(Place an "X" in One Box Only)*

☐ 1 U.S. Government Plaintiff
☐ 3 Federal Question *(U.S. Government Not a Party)*
☐ 2 U.S. Government Defendant
☐ 4 Diversity *(Indicate Citizenship of Parties in Item III)*

III. CITIZENSHIP OF PRINCIPAL PARTIES *(Place an "X" in One Box for Plaintiff and One Box for Defendant)*
(For Diversity Cases Only)

	PTF	DEF		PTF	DEF
Citizen of This State	☐ 1	☐ 1	Incorporated *or* Principal Place of Business In This State	☐ 4	☐ 4
Citizen of Another State	☐ 2	☐ 2	Incorporated *and* Principal Place of Business In Another State	☐ 5	☐ 5
Citizen or Subject of a Foreign Country	☐ 3	☐ 3	Foreign Nation	☐ 6	☐ 6

IV. NATURE OF SUIT *(Place an "X" in One Box Only)*
Click here for: Nature of Suit Code Descriptions.

CONTRACT
☐ 110 Insurance
☐ 120 Marine
☐ 130 Miller Act
☐ 140 Negotiable Instrument
☐ 150 Recovery of Overpayment & Enforcement of Judgment
☐ 151 Medicare Act
☐ 152 Recovery of Defaulted Student Loans (Excludes Veterans)
☐ 153 Recovery of Overpayment of Veteran's Benefits
☐ 160 Stockholders' Suits
☐ 190 Other Contract
☐ 195 Contract Product Liability
☐ 196 Franchise

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

TORTS

PERSONAL INJURY
☐ 310 Airplane
☐ 315 Airplane Product Liability
☐ 320 Assault, Libel & Slander
☐ 330 Federal Employers' Liability
☐ 340 Marine
☐ 345 Marine Product Liability
☐ 350 Motor Vehicle
☐ 355 Motor Vehicle Product Liability
☐ 360 Other Personal Injury
☐ 362 Personal Injury - Medical Malpractice

PERSONAL INJURY
☐ 365 Personal Injury - Product Liability
☐ 367 Health Care/ Pharmaceutical Personal Injury Product Liability
☐ 368 Asbestos Personal Injury Product Liability

PERSONAL PROPERTY
☐ 370 Other Fraud
☐ 371 Truth in Lending
☐ 380 Other Personal Property Damage
☐ 385 Property Damage Product Liability

CIVIL RIGHTS
☐ 440 Other Civil Rights
☐ 441 Voting
☐ 442 Employment
☐ 443 Housing/ Accommodations
☐ 445 Amer. w/Disabilities - Employment
☐ 446 Amer. w/Disabilities - Other
☐ 448 Education

PRISONER PETITIONS
Habeas Corpus:
☐ 463 Alien Detainee
☐ 510 Motions to Vacate Sentence
☐ 530 General
☐ 535 Death Penalty
Other:
☐ 540 Mandamus & Other
☐ 550 Civil Rights
☐ 555 Prison Condition
☐ 560 Civil Detainee - Conditions of Confinement

FORFEITURE/PENALTY
☐ 625 Drug Related Seizure of Property 21 USC 881
☐ 690 Other

LABOR
☐ 710 Fair Labor Standards Act
☐ 720 Labor/Management Relations
☐ 740 Railway Labor Act
☐ 751 Family and Medical Leave Act
☐ 790 Other Labor Litigation
☐ 791 Employee Retirement Income Security Act

IMMIGRATION
☐ 462 Naturalization Application
☐ 465 Other Immigration Actions

BANKRUPTCY
☐ 422 Appeal 28 USC 158
☐ 423 Withdrawal 28 USC 157

INTELLECTUAL PROPERTY RIGHTS
☐ 820 Copyrights
☐ 830 Patent
☐ 835 Patent - Abbreviated New Drug Application
☐ 840 Trademark
☐ 880 Defend Trade Secrets Act of 2016

SOCIAL SECURITY
☐ 861 HIA (1395ff)
☐ 862 Black Lung (923)
☐ 863 DIWC/DIWW (405(g))
☐ 864 SSID Title XVI
☐ 865 RSI (405(g))

FEDERAL TAX SUITS
☐ 870 Taxes (U.S. Plaintiff or Defendant)
☐ 871 IRS—Third Party 26 USC 7609

OTHER STATUTES
☐ 375 False Claims Act
☐ 376 Qui Tam (31 USC 3729(a))
☐ 400 State Reapportionment
☐ 410 Antitrust
☐ 430 Banks and Banking
☐ 450 Commerce
☐ 460 Deportation
☐ 470 Racketeer Influenced and Corrupt Organizations
☐ 480 Consumer Credit (15 USC 1681 or 1692)
☐ 485 Telephone Consumer Protection Act
☐ 490 Cable/Sat TV
☐ 850 Securities/Commodities/ Exchange
☐ 890 Other Statutory Actions
☐ 891 Agricultural Acts
☐ 893 Environmental Matters
☐ 895 Freedom of Information Act
☐ 896 Arbitration
☐ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
☐ 950 Constitutionality of State Statutes

V. ORIGIN *(Place an "X" in One Box Only)*

☐ 1 Original Proceeding
☐ 2 Removed from State Court
☐ 3 Remanded from Appellate Court
☐ 4 Reinstated or Reopened
☐ 5 Transferred from Another District *(specify)*
☐ 6 Multidistrict Litigation - Transfer
☐ 8 Multidistrict Litigation - Direct File

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing ***(Do not cite jurisdictional statutes unless diversity)***:
28 U.S.C. § 1332(d)

Brief description of cause:
Data Breach Litigation

VII. REQUESTED IN COMPLAINT:

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

DEMAND $

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

VIII. RELATED CASE(S) IF ANY

(See instructions): JUDGE ________ DOCKET NUMBER ________

DATE: 06/16/2022
SIGNATURE OF ATTORNEY OF RECORD: /s/ Michael J. Boyle, Jr.

FOR OFFICE USE ONLY

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

INSTRUCTIONS FOR ATTORNEYS COMPLETING CIVIL COVER SHEET FORM JS 44

Authority For Civil Cover Sheet

The JS 44 civil cover sheet and the information contained herein neither replaces nor supplements the filings and service of pleading or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. Consequently, a civil cover sheet is submitted to the Clerk of Court for each civil complaint filed. The attorney filing a case should complete the form as follows:

I.(a) **Plaintiffs-Defendants.** Enter names (last, first, middle initial) of plaintiff and defendant. If the plaintiff or defendant is a government agency, use only the full name or standard abbreviations. If the plaintiff or defendant is an official within a government agency, identify first the agency and then the official, giving both name and title.

(b) **County of Residence.** For each civil case filed, except U.S. plaintiff cases, enter the name of the county where the first listed plaintiff resides at the time of filing. In U.S. plaintiff cases, enter the name of the county in which the first listed defendant resides at the time of filing. (NOTE: In land condemnation cases, the county of residence of the "defendant" is the location of the tract of land involved.)

(c) **Attorneys.** Enter the firm name, address, telephone number, and attorney of record. If there are several attorneys, list them on an attachment, noting in this section "(see attachment)".

II. **Jurisdiction.** The basis of jurisdiction is set forth under Rule 8(a), F.R.Cv.P., which requires that jurisdictions be shown in pleadings. Place an "X" in one of the boxes. If there is more than one basis of jurisdiction, precedence is given in the order shown below.
United States plaintiff. (1) Jurisdiction based on 28 U.S.C. 1345 and 1348. Suits by agencies and officers of the United States are included here.
United States defendant. (2) When the plaintiff is suing the United States, its officers or agencies, place an "X" in this box.
Federal question. (3) This refers to suits under 28 U.S.C. 1331, where jurisdiction arises under the Constitution of the United States, an amendment to the Constitution, an act of Congress or a treaty of the United States. In cases where the U.S. is a party, the U.S. plaintiff or defendant code takes precedence, and box 1 or 2 should be marked.
Diversity of citizenship. (4) This refers to suits under 28 U.S.C. 1332, where parties are citizens of different states. When Box 4 is checked, the citizenship of the different parties must be checked**.** (See Section III below**; NOTE: federal question actions take precedence over diversity cases.**)

III. **Residence (citizenship) of Principal Parties.** This section of the JS 44 is to be completed if diversity of citizenship was indicated above. Mark this section for each principal party.

IV. **Nature of Suit.** Place an "X" in the appropriate box. If there are multiple nature of suit codes associated with the case, pick the nature of suit code that is most applicable. Click here for: Nature of Suit Code Descriptions.

V. **Origin.** Place an "X" in one of the seven boxes.
Original Proceedings. (1) Cases which originate in the United States district courts.
Removed from State Court. (2) Proceedings initiated in state courts may be removed to the district courts under Title 28 U.S.C., Section 1441.
Remanded from Appellate Court. (3) Check this box for cases remanded to the district court for further action. Use the date of remand as the filing date.
Reinstated or Reopened. (4) Check this box for cases reinstated or reopened in the district court. Use the reopening date as the filing date.
Transferred from Another District. (5) For cases transferred under Title 28 U.S.C. Section 1404(a). Do not use this for within district transfers or multidistrict litigation transfers.
Multidistrict Litigation – Transfer. (6) Check this box when a multidistrict case is transferred into the district under authority of Title 28 U.S.C. Section 1407.
Multidistrict Litigation – Direct File. (8) Check this box when a multidistrict case is filed in the same district as the Master MDL docket.
PLEASE NOTE THAT THERE IS NOT AN ORIGIN CODE 7. Origin Code 7 was used for historical records and is no longer relevant due to changes in statute.

VI. **Cause of Action.** Report the civil statute directly related to the cause of action and give a brief description of the cause. **Do not cite jurisdictional statutes unless diversity.** Example: U.S. Civil Statute: 47 USC 553 Brief Description: Unauthorized reception of cable service.

VII. **Requested in Complaint.** Class Action. Place an "X" in this box if you are filing a class action under Rule 23, F.R.Cv.P.
Demand. In this space enter the actual dollar amount being demanded or indicate other demand, such as a preliminary injunction.
Jury Demand. Check the appropriate box to indicate whether or not a jury is being demanded.

VIII. **Related Cases.** This section of the JS 44 is used to reference related pending cases, if any. If there are related pending cases, insert the docket numbers and the corresponding judge names for such cases.

Date and Attorney Signature. Date and sign the civil cover sheet.