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: */s/ Michael J. Boyle, Jr.*

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