Exhibit A3

MEYER WILSON CO., LPA
Matthew R. Wilson (SBN 290473)
mwilson@meyerwilson.com
Michael J. Boyle, Jr. (SBN 258560)
mboyle@meyerwilson.com
305 W. Nationwide Blvd
Columbus, OH 43215
Telephone: (614) 224-6000
Facsimile: (614) 224-6066

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

Attorneys for Plaintiff Robert Grogan and the Proposed Class

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

ROBERT GROGAN and HELENA CRUZ, individually and on behalf of all others similarly situated, Plaintiff, v. MCGRATH RENTCORP Defendant.	Case No. 3:22-cv-00490 **THIRD AMENDED CLASS ACTION COMPLAINT FOR INJUNCTION AND DAMAGES** **Class Action** **JURY TRIAL DEMAND**

Plaintiffs, Robert Grogan and Helena Cruz (“ “Plaintiffs”), through their attorneys, bring this Class Action Complaint against the Defendant, McGrath RentCorp (“MGRC” or “Defendant”), alleging as follows:

I. INTRODUCTION

1. MGRC, a publicly traded company with over 1,000 employees, was a victim of a cybersecurity breach of its employees’ highly sensitive personally identifying information (“PII”) (“Data Breach”). Based on information and belief, MGRC’s security measures were insufficient to safeguard employee PII from the hackers. MGRC disclosed that it lost their PII in

the Data Breach five months after the breach. Mr. Grogan and Ms. Cruz are former MGRC employees and Data Breach victims. Plaintiffs believe that cybercriminals accessed their PII and could have made charges on Mr. Grogan's financial accounts. Plaintiffs bring this Class Action on behalf of themselves and all individuals harmed by MGRC's conduct.

2. MGRC is well-aware it is responsible for safeguarding its employees' highly sensitive PII. Indeed, MGRC tells its employees, investors, and the public that MGRC secures its company data using internal policies, monthly employee training, and "multi-layer cyber protections, including engaging a third-party independent cybersecurity company, who does security testing and monitoring for [the] Company, which includes penetration testing, auditing, and security assessment."[1] On information and belief, MGRC failed to comply with these internal policies and reasonably protect employee data.

3. On July 17, 2021, MGRC discovered that hackers had accessed its systems and employee PII. MGRC reported that the Data Breach caused only "minimal disruption to [its] customer operations," and potentially allowed access to employee "names, addresses, dates of birth, Social Security or individual tax identification numbers, driver's license or other government issued identification card numbers, health-related information, health insurance policy or member numbers, financial account information, and fingerprints."

4. After discovering the Data Breach and quickly restoring its "customer operations," MGRC investigated the breach for five months before informing its employees that their PII were potentially compromised .

5. Because MGRC did not earlier disclose the Data Breach to Plaintiffs, they believe they could not proactively mitigate its impact by securing their data from theft and misuse.

6. In November 2021,upon information and belief, cybercriminals accessed Mr. Grogan's identity used it to make charges to his personal checking account.

[1] *See* MGRC's Privacy Policy, https://www.mgrc.com/eu-general-data-protection-privacy-policy (last visited Jan. 24, 2022).

7. Following its five-month investigation, MGRC disclosed details about the Data Breach. In a notice to its current and former employees on December 15, 2021 ("Breach Notice"), MGRC disclosed that cybercriminals "may" have accessed employee PII.

8. The Breach Notice did not disclose how hackers breached its systems, how many times they were breached, exactly what information was stolen, what MGRC was doing to prevent future breaches, or why it took MGRC five months to issue a bare-bones Breach Notice.

9. Despite the potential harm that the Data Breach poses to its current and former employees, MGRC offered only a one- to two-year credit monitoring service, which plaintiffs do not believe adequately addresses the harm its employees have suffered and will continue to suffer.

10. MGRC's conduct harmed its employees, not only in failing to protect their PII but also in withholding the nature of the Data Breach from its employees, who were unable to proactively protect their identities from theft and misuse.

11. MGRC's failure to protect employees' PII and adequately warn them about the Data Breach violates the law. Plaintiffs are former MGRC employees and Data Breach victims who suffered identity theft and other damages following the hack, causing them to seek relief on a class wide basis.

II. PARTIES

12. Plaintiff, Mr. Grogan, was a citizen and resident of Bakersfield, California from at least November 2014 until approximately November 2021; he is currently a citizen of Georgia. Mr. Grogan is a former MGRC employee, working as an account manager for MGRC's "Adler Tank Rentals" from November 2014 through August 2019. Mr. Grogan was a California resident at all times during his employment with MGRC. Mr. Grogan is a Data Breach victim and received MGRC's Breach Notice to his California address in approximately December 2021.

13. Plaintiff, Ms. Cruz, is a natural person and citizen of this District, residing in Dublin, California, where she intends to remain. Ms. Cruz was a marketing employee of MGRC

from 2013 through 2019.

14. MGRC is a California corporation headquartered at 5700 Las Positas Road, Livermore, California 94551.

15. MGRC does business in California, including in this District.

III. JURISDICTION AND VENUE

16. This Court has jurisdiction over Mr. Grogan's claims under 28 U.S.C. § 1332(d)(2) because there are over 1,000 class members, Mr. Grogan is a citizen of a different state than MGRC, and the aggregate amount in controversy for the class exceeds $5 million, exclusive of interest and costs.

17. The Court has personal jurisdiction over MGRC because MGRC has its principal place of business in this District.

18. Venue is proper in this District under 28 U.S.C. §§ 1391 because a substantial part of the events or omissions giving rise to the claims emanated from activities within this District and Defendant is headquartered in this District.

IV. FACTUAL BACKGROUND

A. MGRC

19. MGRC is a California-based rental company that rents relocatable modular buildings, portable storage containers, electronic test equipment, and liquid and solid containment tanks and boxes" to other businesses.[2] MGRC splits its operations into four divisions: "Mobile Modular," "RTS-RenTelco," "Adler Tanks," and "Enviroplex."

20. MGRC trades on the NASDAQ exchange and, on information and belief, has a $1.8 billion market cap.

21. On information and belief, MGRC employs over 1,000 individuals, with current and former employees living across the United States.

[2] *See* MGRC's 10k report to investors, https://investors.mgrc.com/static-files/b37ae553-0a93-4477-abb3-066a6915db0e (last visited Jan. 17, 2020).

22. MGRC's internal policies recognize MGRC's responsibility for maintaining and securing sensitive data, including employee PII.

23. MGRC's disclosures to its investors recognizes that its failure to maintain adequate cybersecurity protocols could harm MGRC, its investors, and its employees, and "even violate privacy laws:"[3]

Disruptions in our information technology systems or failure to protect these systems against security breaches could adversely affect our business and results of operations. Additionally, if these systems fail, become unavailable for any period of time or are not upgraded, this could limit our ability to effectively monitor and control our operations and adversely affect our operations.

Our information technology systems facilitate our ability to transact business, monitor and control our operations and adjust to changing market conditions. Any disruption in our information technology systems or the failure of these systems to operate as expected could, depending on the magnitude of the problem, adversely affect our operating results by limiting our capacity to effectively transact business, monitor and control our operations and adjust to changing market conditions in a timely manner.

In addition, because of recent advances in technology and well-known efforts on the part of computer hackers and cyber terrorists to breach data security of companies, we face risks associated with potential failure to adequately protect critical corporate, client and employee data, which, if released, could adversely impact our client relationships, our reputation, and even violate privacy laws. As part of our business, we develop, receive and retain confidential data about our company and our customers.

Further, the delay or failure to implement information system upgrades and new systems effectively could disrupt our business, distract management's focus and attention from our business operations and growth initiatives, and increase our implementation and operating costs, any of which could negatively impact our operations and operating results.

24. MGRC's online privacy policy ("Privacy Policy") claims that MGRC employs comprehensive data security protocols to safeguard sensitive data:[4]

To ensure that our employees comply with our privacy policies, we have developed a training program that provides our employees with the tools and knowledge to protect member privacy in all aspects of their work. Any employee who violates our privacy policies is subject to disciplinary action, including possible termination and civil and/or criminal prosecution.

We also take additional cybersecurity measures that include but are not limited to, for example:

- We have a cybersecurity training and testing program that applies to our geographic locations- employees that use technology are required to complete these trainings and testing, which occurs on a regular monthly basis.
- We brief our Board of Directors on cybersecurity on a regular basis (this occurs minimally on an annual basis, with additional discussion as needed).
- We have purchased cybersecurity insurance.
- We comply with PCI-DSS. We have also implemented multi-layer cyber protections, including engaging a third-party independent cybersecurity company, who does security testing and monitoring for our Company, which includes penetration testing, auditing, and security assessment.

[3] *Id.*

[4] *See* MGRC's Privacy Policy: https://www.mgrc.com/eu-general-data-protection-privacy-policy (last visited Jan. 19, 2022).

25. But, on information and belief, MGRC's systems were accessed by cybercriminals that may have leftvulnerabilities in MGRC's systems.

B. MGRC Fails to Safeguard Employee PII

26. Plaintiffs and the proposed Class are current and former MGRC employees.

27. MGRC requires its employees to disclose their PII, including their names, addresses, dates of birth, Social Security or individual tax identification numbers, driver's license or other government issued identification card numbers, as well as health-related information, health insurance policy or member numbers, financial account information, and fingerprints.

28. MGRC collects and maintains employee PII in its computer systems.

29. In collecting and maintaining the PII, MGRC agreed it would safeguard the data according to its internal policies and state and federal law.

30. On July 17, 2021, cybercriminals hacked MGRC's computer systems and accessed employee PII.

31. MGRC allegedly took measures to stop the Data Breach, quickly restoring its "customer operations" to resume business activity. But MGRC informed its current and former employees about the Data Breach five moths later.

32. Four months into MGRC's investigation, on November 15, 2021, MGRC only identified that employees' PII "may" have been accessed by unauthorized users.

33. On December 15, 2021, MGRC disclosed the Data Breach to its current and former employees and state regulators. A true and correct copy of the Breach Notice is attached as **Exhibit A** to this Complaint.

34. Until that time, Plaintiffs and the proposed Class had no idea their PII had been compromised in a data breach and thus could not proactively mitigate the Data Breach's impact on them.

35. The Breach Notice disclaimed any knowledge that employee data was "misused," minimizing the threat that the Data Breach poses to plaintiff and the proposed Class.

36. The Breach Notice then stated, "[n]evertheless, we wanted to inform you of the incident and provide steps you can take to help protect your information[,]" without explaining why MGRC waited five months to do so.

37. The Breach Notice acknowledged the ongoing threat the Data Breach posed to its current and former employees, offering them credit monitoring services. But the "free" services continued for only one to two years.

38. Notably, the Breach Notice did not explain whether MGRC was implementing new cybersecurity protocols to prevent future breaches.

39. On information and belief, MGRC failed to adequately train its employees on reasonable cybersecurity protocols or implement reasonable security measures, causing it to lose control over employee PII. MGRC's alleged negligence is evidenced by its failure to prevent the Data Breach and stop cybercriminals from accessing PII. Further, the Breach Notice makes clear that MGRC it has evidently been unable to determine exactly what information was stolen and when.

C. Plaintiffs' Experience

40. Mr. Grogan was a MGRC employee from November 2014 through August 2019.

41. As a condition of his employment, MGRC required Mr. Grogan to provide his PII.

42. Mr. Grogan provided his PII to MGRC and trusted that the company would use reasonable measures to protect it according to MGRC's internal policies and state and federal law.

43. Following the Data Breach in July 2021, MGRC did not inform Mr. Grogan about the breach, and he did not know that his information had been compromised in the Data Breach.

44. Because MGRC did not immediately disclose the breach, Mr. Grogan was unable

to take precautionary measures earlier, meaning his PII was unprotected for five months until MGRC gave notice.

45. In November 2021, Mr. Grogan suffered identity theft. Mr. Grogan learned that his debit accounts had unauthorized charges at several European locations that he had not visited, and he received notice that his PII had been posted on the dark web.

46. Additionally, Mr. Grogan pays for monthly credit monitoring through Equifax. On approximately January 26, 2022, Mr. Grogan was notified via his MyEquifax account that his social security number had been published on the dark web on a "fraudulent internet trading site."

47. If MGRC had notified Mr. Grogan about the Data Breach earlier, he would have taken precautionary measures sooner and been able to mitigate the effects of the Data Breach on him.

48. Mr. Grogan has spent and will continue to spend considerable time and effort monitoring his accounts to protect himself from additional identity theft. Mr. Grogan fears for his personal financial security and uncertainty over what PII was exposed in the Data Breach. He 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.

49. Further, Mr. Grogan is unsure what has happened to his PII because he does not believe that MGRC has disclosed the true nature of the Data Breach or what measures it is taking to safeguard his PII in the future.

50. MS. Cruz was a MGRC employee from 2013 through 2019.

51. As a condition of her employment, Ms. Cruz provided her PII to McGrath.

52. Ms. Cruz provided her PII and medical information to MGRC and trusted that the company would use reasonable measures to protect it according to MGRC's internal policies and state and federal law.

53. Because MGRC did not immediately disclose the breach to Ms. Cruz, upon information and belief, her PII was unprotected for five months.

54. If MGRC had notified Ms. Cruz about the Data Breach earlier, she would have taken precautionary measures sooner and been able to mitigate the effects of the Data Breach on her.

55. Ms. Cruz has spent and will continue to spend considerable time and effort monitoring her accounts to protect himself from additional identity theft. Ms. Cruz fears for her personal financial security and uncertainty over what PII was exposed in the Data Breach, including her sensitive medical information. She 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.

56. Further, Ms. Cruz is unsure what has happened to her PII because she believes that MGRC has not disclosed the true nature of the Data Breach or what measures it is taking to safeguard her PII in the future.

D. Plaintiffs and the Proposed Class Face Significant Risk of Continued Identity Theft

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

58. As a result of MGRC's failure to prevent the Data Breach, Plaintiffs 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 MGRC and is subject to further breaches so long as MGRC fails to undertake the appropriate measures to protect the PII in their possession.

i. In the case of class members whose health information has been disclosed, such disclosure is itself a significant privacy harm.

59. 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.

60. The value of Plaintiffs' 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. That is what happened to Mr. Grogan in this case.

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

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

63. Cyber-criminals can cross-reference multiple 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.

64. 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 cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiffs and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiffs' and other members of the proposed Class's stolen PII is being misused, and that such misuse is fairly traceable to the Data Breach.

65. Upon information and belief, the attack on MGRC potentially allowed access to the PII of Plaintiffs and members of the proposed Class to people engaged in disruptive and unlawful business practices and tactics, including people who may engage in online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud).

66. MGRC's failure to properly notify Plaintiffs and members of the proposed Class of the Data Breach exacerbated Plaintiffs' 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.

V. CLASS ACTION ALLEGATIONS

67. Plaintiffs sue on behalf of themselves and the proposed Class ("Class"), defined as follows:

All individuals residing in the United States whose PII was compromised in the Data Breach disclosed by MGRC on December 15, 2021.

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

68. Plaintiff Cruz also sues on behalf of herself and the proposed California Subclass, defined as follows:

All individuals residing in California whose PII was compromised in the Data Breach disclosed by MGRC on December 15, 2021.

Excluded from the California Subclass are MGRC, its agents, affiliates, parents, subsidiaries, any entity in which MGRC has a controlling interest, any MGRC officer or director, any successor or assign, and any Judge who adjudicates this case, including their staff and immediate family. Together the Class and the California Subclass are referred to as the "Class."

69. Plaintiffs reserve the right to amend the class definition as discovery progresses.

70. This action satisfies the numerosity, commonality, typicality, and adequacy requirements under Fed. R. Civ. P. 23.

a. **Numerosity**. Plaintiffs are representative of the proposed Class, consisting of over 1,000 members—far too many to join in a single action;

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

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

d. **Adequacy**. Plaintiffs will fairly and adequately protect the proposed Class's interests. Their interests do not conflict with Class members' interests and they

have retained counsel experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf, including as lead counsel.

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

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

ii. Whether MGRC 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 MGRC was negligent in maintaining, protecting, and securing PII;

iv. Whether MGRC breached contract promises to safeguard Plaintiffs' and the Class's PII;

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

vi. Whether MGRC's Breach Notice was reasonable;

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

viii. What the proper damages measure is;

ix. Whether MGRC violated the statutes alleged in this complaint; and

x. Whether Plaintiffs and the Class are entitled to damages, treble damages, or injunctive relief.

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

VI. CAUSES OF ACTION
COUNT I
NEGLIGENCE
(On Behalf of Plaintiffs and the Class)

72. Plaintiffs and members of the Class incorporate the above allegations as if fully set forth herein.

73. Plaintiffs and members of the Class entrusted their PII to Defendant. Defendant owed to Plaintiffs and other members of the Class a duty to exercise reasonable care in handling and using the PII in its care and custody, including 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.

74. Defendant owed a duty of care to Plaintiffs 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 disregard for the security and confidentiality of Plaintiffs' and members of the Class's PII by allegedly not preventing the disclosure of 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 employee who were responsible for making that happen.

75. Defendant owed to Plaintiffs and members of the Class a duty to notify them within a reasonable time frame of any breach to the security of their PII. Defendant also owed a duty to timely and accurately disclose to Plaintiffs and members of the Class the scope, nature, and occurrence of the Data Breach. This duty is required and necessary for Plaintiffs 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.

76. Defendant owed these duties to Plaintiffs 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 Plaintiffs' and members of the Class's personal information and PII as a condition of their employment. Plaintiffs and members of the Class were required to provide their personal information and PII to Defendant to obtain and retain employment with Defendant, and Defendant retained that information.

77. 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.

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

79. Defendant breached its duties by allegedly 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. Defendant further breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiffs and members of the Class, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiffs' and members of the Class's injuries-in-fact. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiffs 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.

80. Indeed, Plaintiffs have suffered identity theft, incurring losses as a result.

81. Defendant's breach of its common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiffs' 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, loss

of privacy, 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 Plaintiffs and the Class)

82. Plaintiffs and members of the Class incorporate the above allegations as if fully set forth herein.

83. 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 Plaintiffs' and members of the Class's PII.

84. 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 Plaintiffs' and the members of the Class's sensitive PII.

85. Upon information and belief, 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 and former employees in the event of a breach, which ultimately came to pass.

86. 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 Plaintiffs and members of the Class.

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

88. Defendant breached its respective duties to Plaintiffs 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 Plaintiffs' and members of the Class's PII.

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

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

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

92. Had Plaintiffs and members of the Class known that Defendant did not adequately protect employees' PII, Plaintiffs and members of the Class would not have entrusted Defendant with their PII.

93. As a direct and proximate result of Defendant's negligence per se, Plaintiffs 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 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; loss of privacy; 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 Plaintiffs and the Class)

94. Plaintiffs and members of the Class incorporate the above allegations as if fully set forth herein.

95. Defendant offered employment to Plaintiffs and members of the Class in exchange for their PII.

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

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

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

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

100. Defendant materially breached the contract(s) it had entered with Plaintiffs and members of the Class by not safeguarding such information from the breach and not providing prompt notice of the intrusion into its computer systems that compromised such information. Defendant further breached the implied contracts with Plaintiffs and members of the Class by:

a. Failing to properly safeguard and protect Plaintiffs 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.

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

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

103. 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.

104. 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.

105. Based on information and belief, plaintiffs believe that Defendant failed to advise Plaintiffs and members of the Class of the Data Breach promptly and sufficiently.

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

107. Plaintiffs 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 Plaintiffs and the Class)

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

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

110. Plaintiffs and members of the Class conferred a benefit upon Defendant in the form of services through employment.

111. Plaintiffs and members of the Class worked for Defendant for a specified rate of remuneration that contemplated Defendant would take adequate safeguards to protect their PII.

112. Defendant appreciated or had knowledge of the benefits conferred upon itself by Plaintiffs and members of the Class. Defendant also benefited from the receipt of Plaintiffs' and members of the Class's PII, as this was used to facilitate their employment.

113. Under principals of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiffs and the proposed Class's services and their PII because Defendant failed to adequately protect their PII. Plaintiffs 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.

114. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiffs 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. Bus. Code § 1798.80, *et seq.*
(On behalf of Plaintiffs and the Class)

115. Plaintiffs incorporate by reference all preceding allegations.

116. 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 § 1798.2.) 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.)

117. The data breach constitutes a "breach of the security system" of Defendant.

118. An unauthorized person acquired the personal, unencrypted information of Plaintiffs and the Class.

119. Five months was an unreasonable delay for providing notice under the circumstances.

120. Upon information and belief, Defendant's unreasonable delay prevented Plaintiffs and the Class from taking appropriate measures from protecting themselves against harm.

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

122. Plaintiffs 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 Plaintiffs and the Class)

123. Plaintiffs incorporate all previous paragraphs as if fully set forth below.

124. 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").

125. Upon information and belief, 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.

126. Upon information and belief, Defendant stored the PII of Plaintiffs 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 Plaintiffs' and the Class's PII secure and prevented the loss or misuse of that

PII.

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

128. Upon information and belief, Defendant also violated California Civil Code § 1798.150 by failing to employ reasonable security measures, resulting in an unauthorized access and exfiltration, theft, or disclosure of Plaintiffs' and the Class's PII.

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

130. Defendant's conduct was unlawful, in that it violated the Consumer Records Act.

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

132. 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.

133. 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.

134. Instead, based on information and belief, Defendant made the PII of Plaintiffs and the Class accessible to scammers, identity thieves, and other malicious actors, subjecting Plaintiffs 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.

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

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

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

138. Therefore, Plaintiffs 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
Declaratory Judgment and Injunctive Relief
(On behalf of Plaintiffs and the Class)

139. Plaintiffs incorporate all previous paragraphs as if fully set forth below.

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

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

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

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

b. Upon information and belief, Defendant breached, and continues to breach, its duty by failing to employ reasonable measures to secure its customers' personal and financial information; and

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

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

144. If an injunction is not issued, Plaintiffs and the Class will suffer irreparable injury and lack an adequate legal remedy in the event of another breach of Defendant's data systems. If another breach of Defendant's data systems occurs, Plaintiffs and the Class will not have an adequate remedy at law because many of the resulting injuries are not readily quantified in full and they will be forced to bring multiple lawsuits to rectify the same conduct. Simply put, monetary damages, while warranted to compensate Plaintiffs and the Class for their out-of-

pocket and other damages that are legally quantifiable and provable, do not cover the full extent of injuries suffered by Plaintiffs and the Class, which include monetary damages that are not legally quantifiable or provable.

145. The hardship to Plaintiffs and the Class if an injunction does not issue exceeds the hardship to Defendant if an injunction is issued.

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

COUNT VIII

Violations of the California Consumer Privacy Act ("CCPA")

CAL. CIV. CODE § 1798.150

(On behalf of Plaintiff Cruz and the California Subclass)

147. Plaintiff Cruz incorporates by reference all preceding allegations.

148. Defendant allegedly violated § 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 Plaintiffs and the California Subclass. As a direct and proximate result, Plaintiff Cruz's believes that the California Subclass's PII was subject to unauthorized access and exfiltration, theft, or disclosure.

149. 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).

150. Plaintiff Cruz and California Subclass 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 Cruz's and California Subclass members' PII. Plaintiff

Cruz and California Subclass members have an interest in ensuring that their PII is reasonably protected.

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

152. 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.

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

VII. PRAYER FOR RELIEF

Plaintiffs 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 Plaintiffs and the proposed Class, appointing Mr. Grogan and Ms. Cruz as class representatives, and appointing their counsel to represent the Class;

B. Awarding declaratory and other equitable relief as is necessary to protect the interests of Plaintiffs and the Class;

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

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

E. Awarding Plaintiffs and the Class damages that include compensatory, exemplary, punitive damages, and statutory damages, including pre- and post-judgment interest, in an amount to be proven at trial;

F. Awarding restitution and damages to Plaintiffs 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 Plaintiffs 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.

VIII. JURY DEMAND

Plaintiffs demand a trial by jury on all issues so triable.

Dated: November 17, 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
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

Attorneys for Plaintiffs and the Proposed Class