

Exhibit A2

1 Matthew R. Wilson (Bar No.290473)
2 Michael J. Boyle, Jr. (Bar No. 258560)
3 MEYER WILSON CO., LPA
4 305 W. Nationwide Blvd.
5 Columbus, OH 43215
6 Telephone: (614) 224-6000
7 Facsimile: (614) 224-6066

8 [Additional counsel appear on signature page]

9 *Attorneys for Plaintiff Robert Grogan and the*
10 *Proposed Class*

11 UNITED STATES DISTRICT COURT
12 NORTHERN DISTRICT OF CALIFORNIA

13 ROBERT GROGAN, individually and on
14 behalf of all others similarly situated,

15 Plaintiff,

16 v.

17 MCGRATH RENTCORP

18 Defendant.

Case No. 3:22-cv-00490

**SECOND AMENDED CLASS ACTION
COMPLAINT FOR INJUNCTION AND
DAMAGES**

Class Action

JURY TRIAL DEMAND

19 Plaintiff, Robert Grogan (“Mr. Grogan” or “Plaintiff”), through his attorneys, brings this
20 Class Action Complaint against the Defendant, McGrath RentCorp (“MGRC” or “Defendant”),
21 alleging as follows:

22 **I. INTRODUCTION**

23 1. MGRC, a publicly traded company with over 1,000 employees, lost control over
24 its employees’ highly sensitive personally identifying information (“PII”) to hackers in a
25 cybersecurity breach (“Data Breach”). Despite recognizing the risk that security breaches pose to
26 MGRC’s employees and its responsibility to quickly warn them about data breaches, MGRC
27 failed to implement reasonable security measures to safeguard employee PII, and then waited
28 five months to disclose that it lost their PII in the Data Breach. In that time, MGRC employees

1 were unable to protect their identities and proactively mitigate the Data Breach’s impact on
2 them. Mr. Grogan is a former MGRC employee and Data Breach victim. In the five months that
3 MGRC waited to disclose the Data Breach, cybercriminals stole Mr. Grogan’s PII, posted it on
4 the dark web, and made charges on his financial accounts. Mr. Grogan brings this Class Action
5 on behalf of himself and all individuals harmed by MGRC’s conduct.

6 2. MGRC is well-aware it is responsible for safeguarding its employees’ highly
7 sensitive PII. Indeed, MGRC tells its employees, investors, and the public that MGRC secures its
8 company data using internal policies, monthly employee training, and “multi-layer cyber
9 protections, including engaging a third-party independent cybersecurity company, who does
10 security testing and monitoring for [the] Company, which includes penetration testing, auditing,
11 and security assessment.”¹ On information and belief, MGRC failed to comply with these
12 internal policies and reasonably protect employee data, leaving employees’ PII an unguarded
13 target for theft and misuse.

14 3. On July 17, 2021, MGRC discovered that hackers had breached its systems and
15 accessed employee PII. Although MGRC says that the Data Breach caused only “minimal
16 disruption to [its] customer operations,” in reality it lost control over employee PII to
17 cybercriminals, allowing criminals access to employee “names, addresses, dates of birth, Social
18 Security or individual tax identification numbers, driver’s license or other government issued
19 identification card numbers, health-related information, health insurance policy or member
20 numbers, financial account information, and fingerprints.”

21 4. Despite discovering the Data Breach and quickly restoring its “customer
22 operations,” MGRC did not immediately inform its employees that their PII was compromised in
23 a security breach. Instead, MGRC “investigated” the breach for *five months* and kept its
24 employees in the dark about its loss of control over their PII.

25 5. Because MGRC did not timely disclose the Data Breach to Mr. Grogan, Mr.

26 ¹ See MGRC’s Privacy Policy, <https://www.mgrc.com/eu-general-data-protection-privacy-policy>
27 (last visited Jan. 24, 2022).

1 Grogan could not proactively mitigate its impact by securing his data from theft and misuse.

2 6. In November 2021—while MGRC was still investigating the Data Breach—
3 cybercriminals stole Mr. Grogan’s identity, posting his PII on the dark web and using it to make
4 charges to his personal checking account.

5 7. Following its five-month “investigation,” MGRC disclosed few details about the
6 Data Breach and the threat it posed. In a notice to its current and former employees on December
7 15, 2021 (“Breach Notice”), MGRC disclosed only that cybercriminals “may” have accessed
8 employee PII, deliberately downplaying the threat the Data Breach posed to its employees.

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

12 9. Despite the lifelong harm that the Data Breach poses to its current and former
13 employees, MGRC offered only a one- to two-year credit monitoring service, which does not
14 adequately address the harm its employees have suffered and will continue to suffer.

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

18 11. MGRC’s failure to protect employees’ PII and adequately warn them about the
19 Data Breach violates the law. Mr. Grogan is a former MGRC employee and Data Breach victim
20 who suffered identity theft following the hack, causing him to seek relief on a class wide basis.

21 **II. PARTIES**

22 12. Plaintiff, Mr. Grogan, was a citizen and resident of Bakersfield, California from at
23 least November 2014 until approximately November 2021; he is currently a citizen of Georgia.
24 Mr. Grogan is a former MGRC employee, working as an account manager for MGRC’s “Adler
25 Tank Rentals” from November 2014 through August 2019. Mr. Grogan was a California resident
26 at all times during his employment with MGRC. Mr. Grogan is a Data Breach victim and
27

1 received MGRC’s Breach Notice to his California address in approximately December 2021.

2 13. MGRC is a California corporation headquartered at 5700 Las Positas Road,
3 Livermore, California 94551.

4 14. MGRC does business in California, including in this District.

5 **III. JURISDICTION AND VENUE**

6 15. This Court has jurisdiction over Mr. Grogan’s claims under 28 U.S.C. §
7 1332(d)(2) because there are over 1,000 class members, Mr. Grogan is a citizen of a different
8 state than MGRC, and the aggregate amount in controversy for the class exceeds \$5 million,
9 exclusive of interest and costs.

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

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

15 **IV. FACTUAL BACKGROUND**

16 **A. MGRC**

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

21 19. MGRC trades on the NASDAQ exchange and, on information and belief, has a
22 \$1.8 billion market cap.

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

25 21. MGRC’s internal policies recognize MGRC’s responsibility for maintaining and

26 ² See MGRC’s 10k report to investors, [https://investors.mgrc.com/static-files/b37ae553-0a93-](https://investors.mgrc.com/static-files/b37ae553-0a93-4477-abb3-066a6915db0e)
27 [4477-abb3-066a6915db0e](https://investors.mgrc.com/static-files/b37ae553-0a93-4477-abb3-066a6915db0e) (last visited Jan. 17, 2020).

1 securing sensitive data, including employee PII.

2 22. MGRC’s disclosures to its investors recognizes that its failure to maintain
3 adequate cybersecurity protocols could harm MGRC, its investors, and its employees, and “even
4 violate privacy laws.”³

5 **Disruptions in our information technology systems or failure to protect these systems against security breaches could adversely affect our business and
6 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.**

7 Our information technology systems facilitate our ability to transact business, monitor and control our operations and adjust to changing market
8 conditions. Any disruption in our information technology systems or the failure of these systems to operate as expected could, depending on the magnitude
9 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.

10 In addition, because of recent advances in technology and well-known efforts on the part of computer hackers and cyber terrorists to breach data
11 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.

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

15 23. MGRC’s online privacy policy (“Privacy Policy”) claims that MGRC employs
16 comprehensive data security protocols to safeguard sensitive data:⁴
17
18
19
20
21
22
23
24

25 ³ *Id.*

26 ⁴ See MGRC’s Privacy Policy: <https://www.mgrc.com/eu-general-data-protection-privacy-policy>
27 (last visited Jan. 19, 2022).

- We brief our board of Directors on cybersecurity on a regular basis (this occurs minimally on an annual basis).
- 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.

1
2 24. But, on information and belief, MGRC fails to strictly adhere to these policies,
3 leaving vulnerabilities in its systems for cybercriminals to exploit.

4 **B. MGRC Fails to Safeguard Employee PII**

5 25. Mr. Grogan and the proposed Class are current and former MGRC employees.

6 26. As a condition of employment with MGRC, MGRC requires its employees to
7 disclose their PII, including their names, addresses, dates of birth, Social Security or individual
8 tax identification numbers, driver’s license or other government issued identification card
9 numbers, as well as health-related information, health insurance policy or member numbers,
10 financial account information, and fingerprints.

11 27. MGRC collects and maintains employee PII in its computer systems.

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

14 29. Despite those commitments, on July 17, 2021, cybercriminals hacked MGRC’s
15 computer systems and accessed employee PII.

16 30. MGRC then supposedly took measures to stop the Data Breach, quickly restoring
17 its “customer operations” to resume business activity. But MGRC took no steps to immediately
18 inform its current and former employees about the Data Breach, choosing instead to
19 “investigate” the breach for five months.

20 31. Four months into MGRC’s investigation, on November 15, 2021, MGRC could
21 only identify that employees’ PII “may” have been accessed by unauthorized users.

22 32. MGRC then waited another month to issue the Breach Notice, on December 15,
23 2021, finally disclosing the Data Breach to its current and former employees and state regulators.
24 A true and correct copy of the Breach Notice is attached as **Exhibit A** to this Complaint.

25 33. Until that time, Mr. Grogan and the proposed Class had no idea their PII had been
26 compromised in a data breach and thus could not proactively mitigate the Data Breach’s impact

1 on them.

2 34. The Breach Notice disclaimed any knowledge that employee data was “misused,”
3 minimizing the threat that the Data Breach poses to plaintiff and the proposed Class.

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

7 36. The Breach Notice acknowledged the ongoing threat the Data Breach posed to its
8 current and former employees, offering them credit monitoring services. But the “free” services
9 continued for only one to two years.

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

12 38. On information and belief, MGRC failed to adequately train its employees on
13 reasonable cybersecurity protocols or implement reasonable security measures, causing it to lose
14 control over employee PII. MGRC’s negligence is evidenced by its failure to prevent the Data
15 Breach and stop cybercriminals from accessing PII. Further, the Breach Notice makes clear that
16 MGRC cannot or will not even determine the full scope of the Data Breach, as it has evidently
17 been unable to determine exactly what information was stolen and when.

18 **C. Plaintiff’s Experience**

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

20 40. As a condition of his employment, MGRC required Mr. Grogan to provide his
21 PII.

22 41. Mr. Grogan provided his PII to MGRC and trusted that the company would use
23 reasonable measures to protect it according to MGRC’s internal policies and state and federal
24 law.

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

1 43. Because MGRC did not immediately disclose the breach, Mr. Grogan was unable
2 to take precautionary measures earlier, meaning his PII was unprotected for five months while
3 MGRC kept its current and former employees in the dark about the breach.

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

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

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

14 47. Mr. Grogan has spent and will continue to spend considerable time and effort
15 monitoring his accounts to protect himself from additional identity theft. Mr. Grogan fears for his
16 personal financial security and uncertainty over what PII was exposed in the Data Breach. He has
17 and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of
18 the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly
19 the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

20 48. Further, Mr. Grogan is unsure what has happened to his PII because MGRC has
21 not disclosed the true nature of the Data Breach or what measures it is taking to safeguard his PII
22 in the future.

23 **D. Plaintiff and the Proposed Class Face Significant Risk of Continued Identity Theft**

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

26 50. As a result of MGRC’s failure to prevent the Data Breach, Plaintiff and the
27

1 proposed Class have suffered and will continue to suffer damages, including monetary losses,
2 lost time, anxiety, and emotional distress. They have suffered or are at an increased risk of
3 suffering:

- 4 a. The loss of the opportunity to control how their PII is used;
- 5 b. The diminution in value of their PII;
- 6 c. The compromise and continuing publication of their PII;
- 7 d. Out-of-pocket costs associated with the prevention, detection, recovery, and
8 remediation from identity theft or fraud;
- 9 e. Lost opportunity costs and lost wages associated with the time and effort
10 expended addressing and attempting to mitigate the actual and future
11 consequences of the Data Breach, including, but not limited to, efforts spent
12 researching how to prevent, detect, contest, and recover from identity theft and
13 fraud;
- 14 f. Delay in receipt of tax refund monies;
- 15 g. Unauthorized use of stolen PII; and
- 16 h. The continued risk to their PII, which remains in the possession of MGRC and is
17 subject to further breaches so long as MGRC fails to undertake the appropriate
18 measures to protect the PII in their possession.
- 19 i. In the case of class members whose health information has been disclosed, such
20 disclosure is itself a significant privacy harm.

21 51. Stolen PII is one of the most valuable commodities on the criminal information
22 black market. According to Experian, a credit-monitoring service, stolen PII can be worth up to
23 \$1,000.00, depending on the type of information obtained.

24 52. The value of Plaintiff’s and the proposed Class’s PII on the black market is
25 considerable. Stolen PII trades on the black market for years, and criminals frequently post stolen
26 private information openly and directly on various “dark web” internet websites, making the
27

1 information publicly available, for a substantial fee of course. That is what happened to Mr.
2 Grogan in this case.

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

5 54. One such example of criminals using PII for profit is the development of “Fullz”
6 packages.

7 55. Cyber-criminals can cross-reference multiple sources of PII to marry unregulated
8 data available elsewhere to criminally stolen data with an astonishingly complete scope and
9 degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are
10 known as “Fullz” packages.

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

21 57. MGRC disclosed the PII of Plaintiff and members of the proposed Class and
22 criminals are using it in the conduct of criminal activity. Specifically, MGRC disclosed and
23 exposed the PII of Plaintiff and members of the proposed Class to people engaged in disruptive
24 and unlawful business practices and tactics, including online account hacking, unauthorized use
25 of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e.,
26 identity fraud), all using the stolen PII.

1 58. MGRC’s failure to properly notify Plaintiff and members of the proposed Class of
2 the Data Breach exacerbated Plaintiff’s and members of the proposed Class’s injury by depriving
3 them of the earliest ability to take appropriate measures to protect their PII and take other
4 necessary steps to mitigate the harm caused by the Data Breach.

5 **V. CLASS ACTION ALLEGATIONS**

6 59. Mr. Grogan sues on behalf of himself and the proposed Class (“Class”), defined
7 as follows:

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

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

13 60. Mr. Grogan reserves the right to amend the class definition as discovery
14 progresses.

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

17 a. **Numerosity**. Mr. Grogan is a representative of the proposed Class,
18 consisting of over 1,000 members—far too many to join in a single action;

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

21 c. **Typicality**. Mr. Grogan’s claims are typical of Class member’s claims as
22 each arises from the same Data Breach, the same alleged negligence and statutory
23 violations by MGRC, and the same unreasonable manner of notifying individuals about
24 the Data Breach.

25 d. **Adequacy**. Mr. Grogan will fairly and adequately protect the proposed
26 Class’s interests. His interests do not conflict with Class members’ interests and he has
27

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

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

- 6 i. Whether MGRC had a duty to use reasonable care in safeguarding Mr.
7 Grogan and the Class's PII;
- 8 ii. Whether MGRC failed to implement and maintain reasonable security
9 procedures and practices appropriate to the nature and scope of the
10 information compromised in the Data Breach;
- 11 iii. Whether MGRC was negligent in maintaining, protecting, and securing
12 PII;
- 13 iv. Whether MGRC breached contract promises to safeguard Mr. Grogan
14 and the Class's PII;
- 15 v. Whether MGRC took reasonable measures to determine the extent of the
16 Data Breach after discovering it;
- 17 vi. Whether MGRC's Breach Notice was reasonable;
- 18 vii. Whether the Data Breach caused Mr. Grogan and the Class injuries;
- 19 viii. What the proper damages measure is;
- 20 ix. Whether MGRC violated the statutes alleged in this complaint; and
- 21 x. Whether Mr. Grogan and the Class are entitled to damages, treble
22 damages, or injunctive relief.

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

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

1
2
3 63. Plaintiff and members of the Class incorporate the above allegations as if fully set
4 forth herein.

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

10 65. Defendant owed a duty of care to Plaintiff and members of the Class because it was
11 foreseeable that Defendant’s failure to adequately safeguard their PII in accordance with state-of-
12 the-art industry standards concerning data security would result in the compromise of that PII—
13 just like the Data Breach that ultimately came to pass. Defendant acted with disregard for the
14 security and confidentiality of Plaintiff’s and members of the Class’s PII by disclosing and
15 providing access to this information to third parties and by failing to properly supervise both the
16 way the PII was stored, used, and exchanged, and those in its employee who were responsible for
17 making that happen.

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

24 67. Defendant owed these duties to Plaintiff and members of the Class because they are
25 members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew
26 or should have known would suffer injury-in-fact from Defendant’s inadequate security protocols.

1 Defendant actively sought and obtained Plaintiff's and members of the Class's personal
2 information and PII as a condition of their employment. Plaintiff and members of the Class were
3 required to provide their personal information and PII to Defendant to obtain and retain
4 employment with Defendant, and Defendant retained that information.

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

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

12 70. Defendant breached its duties by failing to exercise reasonable care in supervising
13 its agents, contractors, vendors, and suppliers, and in handling and securing the personal
14 information and PII of Plaintiff and members of the Class which actually and proximately caused
15 the Data Breach and Plaintiff's and members of the Class's injury. Defendant further breached its
16 duties by failing to provide reasonably timely notice of the Data Breach to Plaintiff and members
17 of the Class, which actually and proximately caused and exacerbated the harm from the Data
18 Breach and Plaintiff's and members of the Class's injuries-in-fact. As a direct and traceable result
19 of Defendant's negligence and/or negligent supervision, Plaintiff and members of the Class have
20 suffered or will suffer damages, including monetary damages, increased risk of future harm,
21 embarrassment, humiliation, frustration, and emotional distress.

22 71. Indeed, Plaintiff has suffered identity theft, incurring losses as a result.

23 72. Defendant's breach of its common-law duties to exercise reasonable care and its
24 failures and negligence actually and proximately caused Plaintiff's and members of the Class
25 actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their PII by
26 criminals, improper disclosure of their PII, lost benefit of their bargain, lost value of their PII, loss
27

1 of privacy, and lost time and money incurred to mitigate and remediate the effects of the Data
2 Breach that resulted from and were caused by Defendant's negligence, which injury-in-fact and
3 damages are ongoing, imminent, immediate, and which they continue to face.

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

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

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

12 75. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce,"
13 including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as
14 Defendant, of failing to use reasonable measures to protect customers or, in this case, employees'
15 PII. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the
16 basis of Defendant's duty to protect Plaintiff and the members of the Class's sensitive PII.

17 76. Defendant violated its duty under Section 5 of the FTC Act by failing to use
18 reasonable measures to protect its employees' PII and not complying with applicable industry
19 standards as described in detail herein. Defendant's conduct was particularly unreasonable given
20 the nature and amount of PII Defendant had collected and stored and the foreseeable consequences
21 of a data breach, including, specifically, the immense damages that would result to its employees
22 and former employees in the event of a breach, which ultimately came to pass.

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

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

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

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

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

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

12 83. Had Plaintiff and members of the Class known that Defendant did not adequately
13 protect employees' PII, Plaintiff and members of the Class would not have entrusted Defendant
14 with their PII.

15 84. As a direct and proximate result of Defendant's negligence per se, Plaintiff
16 members of the Class have suffered harm, including loss of time and money resolving fraudulent
17 charges; loss of time and money obtaining protections against future identity theft;; lost control
18 over the value of PII; unreimbursed losses relating to fraudulent charges; losses relating to
19 exceeding credit and debit card limits and balances; harm resulting from damaged credit scores
20 and information; loss of privacy; and other harm resulting from the unauthorized use or threat of
21 unauthorized use of stolen personal information, entitling them to damages in an amount to be
22 proven at trial.

23 **COUNT III**
24 **Breach of an Implied Contract**
(On Behalf of Plaintiff and the Class)

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

1 110. Defendant knew that an unauthorized person had acquired the personal,
2 unencrypted information of Plaintiffs and the Class, but waited five months to notify them. Five
3 months was an unreasonable delay under the circumstances.

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

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

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

10 **COUNT VI**
Violation of California's Unfair Competition Law
Cal. Bus. Code § 17200, et seq.
(On behalf of Plaintiff and the Class)

12 114. Plaintiff incorporates all previous paragraphs as if fully set forth below.

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

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

19 117. Defendant stored the PII of Plaintiff and the Class in its computer systems and
20 knew or should have known it did not employ reasonable, industry standard, and appropriate
21 security measures that complied with applicable regulations and that would have kept Plaintiff
22 and the Class's PII secure and prevented the loss or misuse of that PII.

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

1 119. Defendant also violated California Civil Code § 1798.150 by failing to employ
2 reasonable security measures, resulting in an unauthorized access and exfiltration, theft, or
3 disclosure of Plaintiff's and the Class's PII.

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

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

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

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

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

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

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

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

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

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

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

14 135. If an injunction is not issued, Plaintiff and the Class will suffer irreparable injury
15 and lack an adequate legal remedy in the event of another breach of Defendant's data systems. If
16 another breach of Defendant's data systems occurs, Plaintiff and the Class will not have an
17 adequate remedy at law because many of the resulting injuries are not readily quantified in full
18 and they will be forced to bring multiple lawsuits to rectify the same conduct. Simply put,
19 monetary damages, while warranted to compensate Plaintiff and the Class for their out-of-pocket
20 and other damages that are legally quantifiable and provable, do not cover the full extent of
21 injuries suffered by Plaintiff and the Class, which include monetary damages that are not legally
22 quantifiable or provable.

23 136. The hardship to Plaintiff and the Class if an injunction does not issue exceeds the
24 hardship to Defendant if an injunction is issued.

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

3 **VIII. JURY DEMAND**

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

5
6 RESPECTFULLY SUBMITTED AND DATED on May 4, 2022.

7 By: /s/ Michael J. Boyle, Jr.

8 Matthew R. Wilson (Bar No. 290473)

9 Email: mwilson@meyerwilson.com

10 Michael J. Boyle, Jr. (Bar No. 258560)

11 Email: mboyle@meyerwilson.com

12 MEYER WILSON CO., LPA

13 305 W. Nationwide Blvd.

14 Columbus, OH 43215

15 Telephone: (614) 224-6000

16 Facsimile: (614) 224-6066

17 Anthony I. Paronich, *Subject to Admission Pro*
18 *Hac Vice*

19 anthony@bparonichlaw.com

20 PARONICH LAW, P.C.

21 350 Lincoln Street, Suite 2400

22 Hingham, Massachusetts 02043

23 Telephone: (617) 485-0018

24 Facsimile: (508) 318-8100

25 Samuel J. Strauss

26 *(Subject to Pro Hac Vice Admission)*

27 Raina Borrelli a

28 *(Subject to Pro Hac Vice Admission)*

TURKE & STRAUSS LLP

613 Williamson St., Suite 201

Madison, WI 53703

Tel: 608-237-1775

sam@turkestrauss.com

raina@turkestrauss.com

Attorneys for Plaintiff and the Proposed Class