

Exhibit A

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. 4:22-cv-00490

**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:

I. INTRODUCTION

22 1. MGRC, a publicly traded company with over 1,000 employees, lost control over
23 its employees’ highly sensitive personally identifying information (“PII”) to hackers in a
24 cybersecurity breach (“Data Breach”). Despite recognizing the risk that security breaches pose to
25 MGRC’s employees and its responsibility to quickly warn them about data breaches, MGRC
26 failed to implement reasonable security measures to safeguard employee PII, and then waited
27 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, is a natural person and citizen of Georgia. Mr. Grogan is a
23 former MGRC employee, working as an account manager for MGRC’s “Adler Tank Rentals”
24 from November 2014 through August 2019. Mr. Grogan is a Data Breach victim and received
25 MGRC’s Breach Notice in December 2021.

26 13. MGRC is a California corporation headquartered at 5700 Las Positas Road,
27
28

1 Livermore, California 94551.

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

3 **III. JURISDICTION AND VENUE**

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

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

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

13 **IV. FACTUAL BACKGROUND**

14 **A. MGRC**

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

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

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

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

25 22. MGRC's disclosures to its investors recognizes that its failure to maintain

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

1 adequate cybersecurity protocols could harm MGRC, its investors, and its employees, and “even
2 violate privacy laws.”³

3 **Disruptions in our information technology systems or failure to protect these systems against security breaches could adversely affect our business and
4 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.**

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

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

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

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

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

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

- 23 • We have a cybersecurity training and testing program that applies to our geographic locations-
24 employees that use technology are required to complete these trainings and testing, which occurs on a
25 regular monthly basis.
- 26 • We brief our Board of Directors on cybersecurity on a regular basis (this occurs minimally on an annual
27 basis, with additional discussion as needed).
- 28 • 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.

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

31 _____
32 ³ *Id.*

33 ⁴ See MGRC’s Privacy Policy: <https://www.mgrc.com/eu-general-data-protection-privacy-policy> (last visited Jan.
34 19, 2022).

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

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

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

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

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

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

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

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

19 32. MGRC then waited another month to issue the Breach Notice, on December 15,
20 2021, finally disclosing the Data Breach to its current and former employees and state regulators.
21 A true and correct copy of the Breach Notice is attached as **Exhibit A** to this Complaint.

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

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

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

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

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

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

15 **C. Plaintiff’s Experience**

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

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

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

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

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

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

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

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

13 47. Further, Mr. Grogan is unsure what has happened to his PII because MGRC has
14 not disclosed the true nature of the Data Breach or what measures it is taking to safeguard his PII
15 in the future.

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

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

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

- 23 a. The loss of the opportunity to control how their PII is used;
- 24 b. The diminution in value of their PII;
- 25 c. The compromise and continuing publication of their PII;
- 26 d. Out-of-pocket costs associated with the prevention, detection, recovery, and

1 remediation from identity theft or fraud;

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

7 f. Delay in receipt of tax refund monies;

8 g. Unauthorized use of stolen PII; and

9 h. The continued risk to their PII, which remains in the possession of MGRC and is
10 subject to further breaches so long as MGRC fails to undertake the appropriate
11 measures to protect the PII in their possession.

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

14 50. Stolen PII is one of the most valuable commodities on the criminal information
15 black market. According to Experian, a credit-monitoring service, stolen PII can be worth up to
16 \$1,000.00, depending on the type of information obtained.

17 51. The value of Plaintiff's and the proposed Class's PII on the black market is
18 considerable. Stolen PII trades on the black market for years, and criminals frequently post stolen
19 private information openly and directly on various "dark web" internet websites, making the
20 information publicly available, for a substantial fee of course. That is what happened to Mr.
21 Grogan in this case.

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

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

26 54. Cyber-criminals can cross-reference multiple sources of PII to marry unregulated
27

1 data available elsewhere to criminally stolen data with an astonishingly complete scope and
2 degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are
3 known as “Fullz” packages.

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

14 56. MGRC disclosed the PII of Plaintiff and members of the proposed Class and
15 criminals are using it in the conduct of criminal activity. Specifically, MGRC disclosed and
16 exposed the PII of Plaintiff and members of the proposed Class to people engaged in disruptive
17 and unlawful business practices and tactics, including online account hacking, unauthorized use
18 of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e.,
19 identity fraud), all using the stolen PII.

20 57. MGRC’s failure to properly notify Plaintiff and members of the proposed Class of
21 the Data Breach exacerbated Plaintiff’s and members of the proposed Class’s injury by depriving
22 them of the earliest ability to take appropriate measures to protect their PII and take other
23 necessary steps to mitigate the harm caused by the Data Breach.

24 **V. CLASS ACTION ALLEGATIONS**

25 58. Mr. Grogan sues on behalf of himself and the proposed Class (“Class”), defined
26 as follows:

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

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

6 59. Mr. Grogan reserves the right to amend the class definition as discovery
7 progresses.

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

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

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

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

18 d. **Adequacy**. Mr. Grogan will fairly and adequately protect the proposed
19 Class’s interests. His interests do not conflict with Class members’ interests and he has
20 retained counsel experienced in complex class action litigation and data privacy to
21 prosecute this action on the Class’s behalf, including as lead counsel.

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

25 i. Whether MGRC had a duty to use reasonable care in safeguarding Mr.
26 Grogan and the Class’s PII;

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

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

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

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

25 63. Plaintiff and members of the Class entrusted their PII to Defendant. Defendant
 26 owed to Plaintiff and other members of the Class a duty to exercise reasonable care in handling
 27 and using the PII in its care and custody, including implementing industry-standard security

1 procedures sufficient to reasonably protect the information from the Data Breach, theft, and
2 unauthorized use that came to pass, and to promptly detect attempts at unauthorized access.

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

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

17 66. Defendant owed these duties to Plaintiff and members of the Class because they are
18 members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew
19 or should have known would suffer injury-in-fact from Defendant’s inadequate security protocols.
20 Defendant actively sought and obtained Plaintiff’s and members of the Class’s personal
21 information and PII for addiction-related treatment services. Plaintiff and members of the Class
22 were required to provide their personal information and PII to Defendant to receive those
23 addiction-related treatment services from Defendant, and Defendant retained that information.

24 67. The risk that unauthorized persons would attempt to gain access to the PII and
25 misuse it was foreseeable. Given that Defendant holds vast amounts of PII, it was inevitable that
26
27
28

1 unauthorized individuals would attempt to access Defendant's databases containing the PII—
2 whether by malware or otherwise.

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

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

16 70. Indeed, Plaintiff has suffered identity theft, incurring losses as a result.

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

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

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

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

4 74. Section 5 of the FTC Act prohibits “unfair . . . practices in or affecting commerce,”
5 including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as
6 Defendant, of failing to use reasonable measures to protect customers or, in this case, patients’ PII.
7 The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis
8 of Defendant’s duty to protect Plaintiff and the members of the Class’s sensitive PII.

9 75. Defendant violated its duty under Section 5 of the FTC Act by failing to use
10 reasonable measures to protect its patients’ PII and not complying with applicable industry
11 standards as described in detail herein. Defendant’s conduct was particularly unreasonable given
12 the nature and amount of PII Defendant had collected and stored and the foreseeable consequences
13 of a data breach, including, specifically, the immense damages that would result to its employees
14 and former employees in the event of a breach, which ultimately came to pass.

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

19 77. Defendant had a duty to Plaintiff and the members of the Class to implement and
20 maintain reasonable security procedures and practices to safeguard Plaintiff’s and the Class’s PII.

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

24 79. Defendant’s violation of Section 5 of the FTC Act and its failure to comply with
25 applicable laws and regulations constitutes negligence per se.

26
27
28

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

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

7 82. Had Plaintiff and members of the Class known that Defendant did not adequately
8 protect patients’ PII, Plaintiff and members of the Class would not have entrusted Defendant with
9 their PII.

10 83. As a direct and proximate result of Defendant’s negligence per se, Plaintiff
11 members of the Class have suffered harm, including loss of time and money resolving fraudulent
12 charges; loss of time and money obtaining protections against future identity theft; financial losses
13 related to the treatment Plaintiff and members of the Class paid for that they would not have
14 received had they known of Defendant’s careless approach to cyber security; lost control over the
15 value of PII; unreimbursed losses relating to fraudulent charges; losses relating to exceeding credit
16 and debit card limits and balances; harm resulting from damaged credit scores and information;
17 loss of privacy; and other harm resulting from the unauthorized use or threat of unauthorized use
18 of stolen personal information, entitling them to damages in an amount to be proven at trial.

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

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

23 85. Defendant offered employment to Plaintiff and members of the Class in exchange
24 for their PII.

25
26
27

1 honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection
2 with executing contracts and discharging performance and other duties according to their terms,
3 means preserving the spirit—not merely the letter—of the bargain. Put differently, the parties to a
4 contract are mutually obligated to comply with the substance of their contract in addition to its
5 form.

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

9 95. Defendant failed to advise Plaintiff and members of the Class of the Data Breach
10 promptly and sufficiently.

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

12 97. Plaintiff and members of the Class have sustained damages because of Defendant’s
13 breaches of its agreement, including breaches thereof through violations of the covenant of good
14 faith and fair dealing.

15 **COUNT IV**
16 **Unjust Enrichment**
(On Behalf of Plaintiff and the Class)

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

19 99. This claim is pleaded in the alternative to the breach of implied contractual duty
20 claim.

21 100. Plaintiff and members of the Class conferred a benefit upon Defendant in the form
22 of services through employment.

23 101. Plaintiff and members of the Class worked for Defendant for a specified rate of
24 remuneration that contemplated Defendant would take adequate safeguards to protect their PII.

1 102. Defendant appreciated or had knowledge of the benefits conferred upon itself by
2 Plaintiff and members of the Class. Defendant also benefited from the receipt of Plaintiff’s and
3 members of the Class’s PII, as this was used to facilitate their employment.

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

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

COUNT V
Violation of California’s Consumer Records Act
Cal. Bus. Code § 1798.80, et seq.
(On behalf of Plaintiff and the Class)

14 105. Plaintiff incorporates by reference all preceding allegations.

15 106. Under California law, any “person or business that conducts business in
16 California, and that owns or licenses computerized data that includes personal information” must
17 “disclose any breach of the system following discovery or notification of the breach in the
18 security of the data to any resident of California whose unencrypted personal information was, or
19 is reasonably believed to have been, acquired by an unauthorized person.” (CAL. CIV. CODE §
20 1798.2.) The disclosure must “be made in the most expedient time possible and without
21 unreasonable delay” (*Id.*), but “immediately following discovery [of the breach], if the personal
22 information was, or is reasonably believed to have been, acquired by an unauthorized person.”
23 (CAL. CIV. CODE § 1798.82, subdiv. b.)

24 107. The data breach constitutes a “breach of the security system” of Defendant.

25 108. An unauthorized person acquired the personal, unencrypted information of
26 Plaintiff and the Class.

27
28

1 118. 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.

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

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

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

9 122. 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.

13 123. 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.

23 124. 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.

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

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

5 127. There were reasonably available alternatives to further Defendant’s legitimate
6 business interests, other than the misconduct alleged in this complaint.

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

12 **COUNT VII**
13 **Declaratory Judgment and Injunctive Relief**
14 **(On behalf of Plaintiff and the Class)**

15 129. Plaintiff incorporates all previous paragraphs as if fully set forth below.

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

21 131. An actual controversy has arisen in the wake of the Data Breach at issue regarding
22 Defendant’s common law and other duties to act reasonably with respect to employing
23 reasonable data security. Plaintiff alleges Defendant’s actions in this respect were inadequate and
24 unreasonable and, upon information and belief, remain inadequate and unreasonable.
25 Additionally, Plaintiff and the Class continue to suffer injury due to the continued and ongoing
26 threat of new or additional fraud against them or on their accounts using the stolen data.
27
28

1 132. 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 healthcare and financial records it obtains from its clients, and to notify impacted individuals
6 of the Data 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.

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

14 134. 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.

23 135. 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 January 25, 2022.

7 By: /s/

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 *Attorneys for Plaintiff and the Proposed Class*

EXHIBIT A



P.O. Box 1907
Suwanee, GA 30024

To Enroll, Please Call:
1-833-381-2286
Or Visit:
<https://app.idx.us/account-creation/protect>
Enrollment Code: [XXXXXXXXXX]

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

December 15, 2021

Re: <<Variable Field 1>>

Dear <<First Name>> <<Last Name>>,

We are writing to inform you of an incident that may have involved your personal information. At McGrath RentCorp (“MGRC”), we take the privacy and security of your information very seriously. Therefore, we are writing to inform you of the incident, advising you of certain steps you can take to help protect your personal information, and offering complementary identity monitoring services at no cost to you to further guard your information.

What Happened? On July 17, 2021, MGRC discovered unauthorized activity on its systems by an unknown actor. In response, we took the systems offline to stop the unauthorized access and worked with our cybersecurity experts to further examine the incident. All services have since been restored, and the incident caused minimal disruption to our customer operations.

Since then, we have been working diligently to assess what information may have been impacted. On November 15, 2021, MGRC determined that the data involved included information relating to you.

We have no indication that any information has been misused as a result of this incident. Nevertheless, we wanted to inform you of the incident and provide steps you can take to help protect your information.

What Information Was Involved? The files that may have been accessed by the unauthorized individual generally contained the following information: 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. Please note that the information affected varied from person-to-person.

What Are We Doing? As soon as we discovered the incident, we took the steps described above. We also reported the incident to the Federal Bureau of Investigation and will provide whatever cooperation is necessary to help identify and prosecute the perpetrators.

In addition, we have secured the services of IDX to provide identity protection services at no cost to you. IDX is a risk mitigation and response vendor and has extensive experience helping people who have sustained an unintentional exposure of confidential data. The services include credit monitoring, Cyberscan dark web monitoring, \$1 million identity theft reimbursement insurance, and fully managed identity recovery services for <<12 or 24 months>>.

To receive these services, you must be over the age of 18, have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

McGrath RentCorp
5700 Las Positas Rd, Livermore, CA 94551

You can enroll by going to <https://app.idx.us/account-creation/protect> or calling IDX at 1-833-381-2286 and using the Enrollment Code provided at the top of this letter. Please note that the deadline to enroll is March 15, 2022.

What You Can Do: Please review the “Steps You Can Take to Further Protect Your Information” sheet included with this letter. It describes additional ways you can help safeguard your information. We also encourage you to enroll in the complimentary identity monitoring services we are offering through IDX.

For More Information: If you have questions or need assistance, please call 1-833-381-2286, Monday through Friday from 6 a.m. to 6 p.m. Pacific.

Protecting your information is important to us. Please know that we take this incident very seriously and deeply regret any worry or inconvenience that this may cause you.

Sincerely,

A handwritten signature in black ink, appearing to read 'JF Hanna', with a long horizontal stroke extending to the right.

Joseph F. Hanna
CEO

Steps You Can Take to Further Protect Your Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com/>, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print this form at <https://www.annualcreditreport.com/cra/requestformfinal.pdf>. You also can contact one of the following three national credit reporting agencies:

TransUnion	Experian	Equifax	Free Annual Report
P.O. Box 1000	P.O. Box 9532	P.O. Box 105851	P.O. Box 105281
Chester, PA19016	Allen, TX 75013	Atlanta, GA 30348	Atlanta, GA 30348
1-800-909-8872	1-888-397-3742	1-800-685-1111	1-877-322-8228
www.transunion.com	www.experian.com	www.equifax.com	www.annualcreditreport.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>.

Security Freeze: Under U.S. law, you have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state. Contact information for the FTC is: **Federal Trade Commission**, 600 Pennsylvania Ave, NW, Washington, DC 20580, www.consumer.ftc.gov and www.ftc.gov/idtheft, 1-877-438-4338. Residents of New York, Maryland, North Carolina, and Rhode Island can obtain more information from their Attorneys General using the contact information below.

New York Attorney General Bureau of Internet and Technology Resources	Maryland Attorney General	North Carolina Attorney General	Rhode Island Attorney General
28 Liberty Street New York, NY 10005 ifraud@ag.ny.gov 1-212-416-8433	200 St. Paul Place Baltimore, MD 21202 www.oag.state.md.us 1-888-743-0023	9001 Mail Service Center Raleigh, NC 27699 www.ncdoj.gov 1-877-566-7226	150 South Main Street Providence, RI 02903 www.riag.ri.gov 401-274-4400

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information, as well as others. For more information about the FCRA, and your rights pursuant to the FCRA, please visit http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.

CIVIL COVER SHEET

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

I. (a) PLAINTIFFS

ROBERT GROGAN, individually and on behalf of a class

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

(c) Attorneys (Firm Name, Address, and Telephone Number)

Michael Boyle, Meyer Wilson Co., LPA, 305 W. Nationwide Blvd., Columbus, OH 43215, 614-224-6000

DEFENDANTS

McGrath RentCorp.

County of Residence of First Listed Defendant Alameda (IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys (If Known)

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

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

III. CITIZENSHIP OF PRINCIPAL PARTIES (Place an "X" in One Box for Plaintiff and One Box for Defendant)

Table with columns for Plaintiff (PTF) and Defendant (DEF) citizenship and incorporation status.

IV. NATURE OF SUIT (Place an "X" in One Box Only)

Large table with categories: CONTRACT, REAL PROPERTY, TORTS, CIVIL RIGHTS, PRISONER PETITIONS, HABEAS CORPUS, FORFEITURE/PENALTY, LABOR, IMMIGRATION, BANKRUPTCY, SOCIAL SECURITY, FEDERAL TAX SUITS, OTHER STATUTES.

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

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

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing (Do not cite jurisdictional statutes unless diversity): 28 U.S.C. s 1332(d)(2)

Brief description of cause:

Claims arising from a negligent data breach of employee Personal Identifying Information

VII. REQUESTED IN COMPLAINT:

CHECK IF THIS IS A CLASS ACTION UNDER RULE 23, Fed. R. Civ. P. DEMAND \$ 5,000,000.00 CHECK YES only if demanded in complaint: JURY DEMAND: X Yes No

VIII. RELATED CASE(S), IF ANY (See instructions):

JUDGE DOCKET NUMBER

IX. DIVISIONAL ASSIGNMENT (Civil Local Rule 3-2)

(Place an "X" in One Box Only) X SAN FRANCISCO/OAKLAND SAN JOSE EUREKA-MCKINLEYVILLE

DATE 01/25/2022

SIGNATURE OF ATTORNEY OF RECORD

/s/ Michael J. Boyle, Jr.

INSTRUCTIONS FOR ATTORNEYS COMPLETING CIVIL COVER SHEET FORM JS-CAND 44

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

- I. a) Plaintiffs-Defendants.** Enter names (last, first, middle initial) of plaintiff and defendant. If the plaintiff or defendant is a government agency, use only the full name or standard abbreviations. If the plaintiff or defendant is an official within a government agency, identify first the agency and then the official, giving both name and title.
 - b) County of Residence.** For each civil case filed, except U.S. plaintiff cases, enter the name of the county where the first listed plaintiff resides at the time of filing. In U.S. plaintiff cases, enter the name of the county in which the first listed defendant resides at the time of filing. (NOTE: In land condemnation cases, the county of residence of the “defendant” is the location of the tract of land involved.)
 - c) Attorneys.** Enter the firm name, address, telephone number, and attorney of record. If there are several attorneys, list them on an attachment, noting in this section “(see attachment).”
- II. Jurisdiction.** The basis of jurisdiction is set forth under Federal Rule of Civil Procedure 8(a), which requires that jurisdictions be shown in pleadings. Place an “X” in one of the boxes. If there is more than one basis of jurisdiction, precedence is given in the order shown below.
- (1) United States plaintiff. Jurisdiction based on 28 USC §§ 1345 and 1348. Suits by agencies and officers of the United States are included here.
 - (2) United States defendant. When the plaintiff is suing the United States, its officers or agencies, place an “X” in this box.
 - (3) Federal question. This refers to suits under 28 USC § 1331, where jurisdiction arises under the Constitution of the United States, an amendment to the Constitution, an act of Congress or a treaty of the United States. In cases where the U.S. is a party, the U.S. plaintiff or defendant code takes precedence, and box 1 or 2 should be marked.
 - (4) Diversity of citizenship. This refers to suits under 28 USC § 1332, where parties are citizens of different states. When Box 4 is checked, the citizenship of the different parties must be checked. (See Section III below; **NOTE: federal question actions take precedence over diversity cases.**)
- III. Residence (citizenship) of Principal Parties.** This section of the JS-CAND 44 is to be completed if diversity of citizenship was indicated above. Mark this section for each principal party.
- IV. Nature of Suit.** Place an “X” in the appropriate box. If the nature of suit cannot be determined, be sure the cause of action, in Section VI below, is sufficient to enable the deputy clerk or the statistical clerk(s) in the Administrative Office to determine the nature of suit. If the cause fits more than one nature of suit, select the most definitive.
- V. Origin.** Place an “X” in one of the six boxes.
- (1) Original Proceedings. Cases originating in the United States district courts.
 - (2) Removed from State Court. Proceedings initiated in state courts may be removed to the district courts under Title 28 USC § 1441. When the petition for removal is granted, check this box.
 - (3) Remanded from Appellate Court. Check this box for cases remanded to the district court for further action. Use the date of remand as the filing date.
 - (4) Reinstated or Reopened. Check this box for cases reinstated or reopened in the district court. Use the reopening date as the filing date.
 - (5) Transferred from Another District. For cases transferred under Title 28 USC § 1404(a). Do not use this for within district transfers or multidistrict litigation transfers.
 - (6) Multidistrict Litigation Transfer. Check this box when a multidistrict case is transferred into the district under authority of Title 28 USC § 1407. When this box is checked, do not check (5) above.
 - (8) Multidistrict Litigation Direct File. Check this box when a multidistrict litigation case is filed in the same district as the Master MDL docket. Please note that there is no Origin Code 7. Origin Code 7 was used for historical records and is no longer relevant due to changes in statute.
- VI. Cause of Action.** Report the civil statute directly related to the cause of action and give a brief description of the cause. **Do not cite jurisdictional statutes unless diversity.** Example: U.S. Civil Statute: 47 USC § 553. Brief Description: Unauthorized reception of cable service.
- VII. Requested in Complaint.** Class Action. Place an “X” in this box if you are filing a class action under Federal Rule of Civil Procedure 23. Demand. In this space enter the actual dollar amount being demanded or indicate other demand, such as a preliminary injunction. Jury Demand. Check the appropriate box to indicate whether or not a jury is being demanded.
- VIII. Related Cases.** This section of the JS-CAND 44 is used to identify related pending cases, if any. If there are related pending cases, insert the docket numbers and the corresponding judge names for such cases.
- IX. Divisional Assignment.** If the Nature of Suit is under Property Rights or Prisoner Petitions or the matter is a Securities Class Action, leave this section blank. For all other cases, identify the divisional venue according to Civil Local Rule 3-2: “the county in which a substantial part of the events or omissions which give rise to the claim occurred or in which a substantial part of the property that is the subject of the action is situated.”
- Date and Attorney Signature.** Date and sign the civil cover sheet.



P.O. Box 1907
Suwanee, GA 30024

To Enroll, Please Call:
1-833-381-2286
Or Visit:
<https://app.idx.us/account-creation/protect>
Enrollment Code: [XXXXXXXXXX]

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

December 15, 2021

Re: <<Variable Field 1>>

Dear <<First Name>> <<Last Name>>,

We are writing to inform you of an incident that may have involved your personal information. At McGrath RentCorp (“MGRC”), we take the privacy and security of your information very seriously. Therefore, we are writing to inform you of the incident, advising you of certain steps you can take to help protect your personal information, and offering complementary identity monitoring services at no cost to you to further guard your information.

What Happened? On July 17, 2021, MGRC discovered unauthorized activity on its systems by an unknown actor. In response, we took the systems offline to stop the unauthorized access and worked with our cybersecurity experts to further examine the incident. All services have since been restored, and the incident caused minimal disruption to our customer operations.

Since then, we have been working diligently to assess what information may have been impacted. On November 15, 2021, MGRC determined that the data involved included information relating to you.

We have no indication that any information has been misused as a result of this incident. Nevertheless, we wanted to inform you of the incident and provide steps you can take to help protect your information.

What Information Was Involved? The files that may have been accessed by the unauthorized individual generally contained the following information: 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. Please note that the information affected varied from person-to-person.

What Are We Doing? As soon as we discovered the incident, we took the steps described above. We also reported the incident to the Federal Bureau of Investigation and will provide whatever cooperation is necessary to help identify and prosecute the perpetrators.

In addition, we have secured the services of IDX to provide identity protection services at no cost to you. IDX is a risk mitigation and response vendor and has extensive experience helping people who have sustained an unintentional exposure of confidential data. The services include credit monitoring, Cyberscan dark web monitoring, \$1 million identity theft reimbursement insurance, and fully managed identity recovery services for <<12 or 24 months>>.

To receive these services, you must be over the age of 18, have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

McGrath RentCorp
5700 Las Positas Rd, Livermore, CA 94551

You can enroll by going to <https://app.idx.us/account-creation/protect> or calling IDX at 1-833-381-2286 and using the Enrollment Code provided at the top of this letter. Please note that the deadline to enroll is March 15, 2022.

What You Can Do: Please review the “Steps You Can Take to Further Protect Your Information” sheet included with this letter. It describes additional ways you can help safeguard your information. We also encourage you to enroll in the complimentary identity monitoring services we are offering through IDX.

For More Information: If you have questions or need assistance, please call 1-833-381-2286, Monday through Friday from 6 a.m. to 6 p.m. Pacific.

Protecting your information is important to us. Please know that we take this incident very seriously and deeply regret any worry or inconvenience that this may cause you.

Sincerely,

A handwritten signature in black ink, appearing to be 'JF Hanna', written over a horizontal line.

Joseph F. Hanna
CEO

Steps You Can Take to Further Protect Your Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com/>, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print this form at <https://www.annualcreditreport.com/cra/requestformfinal.pdf>. You also can contact one of the following three national credit reporting agencies:

TransUnion	Experian	Equifax	Free Annual Report
P.O. Box 1000	P.O. Box 9532	P.O. Box 105851	P.O. Box 105281
Chester, PA19016	Allen, TX 75013	Atlanta, GA 30348	Atlanta, GA 30348
1-800-909-8872	1-888-397-3742	1-800-685-1111	1-877-322-8228
www.transunion.com	www.experian.com	www.equifax.com	www.annualcreditreport.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>.

Security Freeze: Under U.S. law, you have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state. Contact information for the FTC is: **Federal Trade Commission**, 600 Pennsylvania Ave, NW, Washington, DC 20580, www.consumer.ftc.gov and www.ftc.gov/idtheft, 1-877-438-4338. Residents of New York, Maryland, North Carolina, and Rhode Island can obtain more information from their Attorneys General using the contact information below.

New York Attorney General Bureau of Internet and Technology Resources	Maryland Attorney General	North Carolina Attorney General	Rhode Island Attorney General
28 Liberty Street New York, NY 10005 ifraud@ag.ny.gov 1-212-416-8433	200 St. Paul Place Baltimore, MD 21202 www.oag.state.md.us 1-888-743-0023	9001 Mail Service Center Raleigh, NC 27699 www.ncdoj.gov 1-877-566-7226	150 South Main Street Providence, RI 02903 www.riag.ri.gov 401-274-4400

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information, as well as others. For more information about the FCRA, and your rights pursuant to the FCRA, please visit http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.